CONFIABILIDADE DE SISTEMAS INSTRUMENTADOS DE SEGURANÇA: ANÁLISE CUSTO-BENEFÍCIO DE ALTERNATIVAS PARA O ATENDIMENTO AO SIL REQUERIDO EM INSTALAÇÕES INDUSTRIAIS

Luciana Moreira Chame

DISSERTAÇÃO SUBMETIDA AO CORPO DOCENTE DA COORDENAÇÃO DOS PROGRAMAS DE PÓS-GRADUAÇÃO DE ENGENHARIA DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE EM CIÊNCIAS EM ENGENHARIA DE PRODUÇÃO.

Aprovada por:

Prof. Basílio de Bragança Pereira, Ph.D.

Prof. Paulo Fernando Ferreira Frutuoso e Melo, D.Sc.

Prof. Virgílio José Martins Ferreira Filho, D.Sc.

Dr. Luiz Fernando Seixas de Oliveira, Ph.D.

RIO DE JANEIRO, RJ - BRASIL

MAIO DE 2007

CHAME, LUCIANA MOREIRA

Confiabilidade de Sistemas Instrumentados de Segurança: Análise Custo-Benefício de Alternativas para o Atendimento ao SIL Requerido em Instalações Industriais [Rio de Janeiro] 2007

XV, 167 p. 29,7 cm (COPPE/UFRJ, M.Sc., Engenharia de Produção, 2007)

Dissertação - Universidade Federal do Rio de Janeiro, COPPE

1. SIL
2. Sistemas Instrumentados de Segurança
3. Confiabilidade de Sistemas
4. PFD

I. COPPE/UFRJ II. Título (série)

*Dedico este trabalho para minha avó* ***Maria da Conceição****, que sempre me acompanhou e incentivou em tudo que eu já fiz na vida e que gostaria que estivesse neste momento aqui para ver mais esta etapa concluída.*

*Para* ***Guilherme****, meu sobrinho, minha VIDA e minha alegria de viver.*

# Agradecimentos

Gostaria de agradecer àqueles que diretamente ou indiretamente colaboraram para a realização deste meu trabalho, em especial:

- A Deus: princípio, meio e fim.

- Ao orientador, chefe, mestre e amigo, **Luiz Fernando Seixas de Oliveira** por todo apoio, orientação, incentivo, cobrança e ajuda em todos os pequenos e grandes detalhes, fundamentais para a realização deste trabalho, bem como pela oportunidade diária de aprendizado com um pioneiro da Engenharia de Confiabilidade no Brasil.

- Ao Professor **Paulo Fernando Frutuoso Ferreira e Melo** por ter aceito a orientação deste trabalho e por todo o apoio e incentivo prestados, tornando todo este processo extremamente agradável.

- Ao Professor **Basílio de Bragança Pereira** por ter aceito a orientação deste trabalho e pela participação na banca examinadora.

- Ao Professor **Virgílio José Martins Ferreira Filho**, por ter aceito fazer parte da banca examinadora, pelas sugestões, incentivo e apoio, durante todo o período de realização do mestrado.

- Aos adoráveis amigos que fiz durante o mestrado: **Debora**, **Wagner**, **Renato**, **Samuel**, **Maria**, **Victor**, **Geiza** e **Vinícius**, pelas noites e intermináveis fins de semana dedicados ao estudo, pelos aconselhamentos e pela verdadeira amizade. Em particular agradeço aos amigos **Debora** e **Wagner**, pelo acompanhamento quase que diário da elaboração desta dissertação, com palavras de apoio e incen-

tivo, além de principalmente muita paciência para os momentos de angústia e quase "desespero" com prazos e problemas com o LaTex.

- À secretária do Departamento de Pesquisa Operacional **Andréia Lima da Silva Moreira**, pela simpatia e incansável ajuda em todos os momentos.

- À **DNV** pelo constante apoio e por ceder computador, seus programas computacionais (principalmente o ORBIT SIL) e referências bibliográficas, imprescindíveis para o desenvolvimento deste trabalho.

- A todos os **amigos da DNV** (Rio de Janeiro, São Paulo, Salvador, Porto Alegre e Buenos Aires) pelo apoio, incentivo e exemplo de profissionalismo e competência, com o qual tenho tido o prazer de conviver nestes últimos 7 anos de minha vida profissional e acadêmica. Em particular, gostaria de agradecer ao amigo **Sávio**, pelo incentivo e orientação para a escolha da instituição e do curso realizado; ao gerente e amigo **Flávio**, pelo apoio que tornou possível a conclusão deste curso; e aos amigos de hoje e sempre **Nilda**, **Marcelo**, **Tobias**, **Mariana**, **Sandro**, **Ana Cristina**, **Jaime**, **Cássia**, **João Paulo**, **João Vicente**, **Felipe**, **Galvão**, **Daniel**, **João Carlos**, **Paula**, **Gladys**, **Hélio**, **Joaquim**, **Paradela**, **Geraldo**, **Eduardo**, **Pedro**, **Ricardo**, **Flávia**, **Gustavo**, **Marcela**, **Darío**, **César**, **Lopes**, **Tatiana**, **Rosemeire**, **Santux**, **Marcus**, **Carlos Eduardo**, **Diogo**, **Fernando**, **Helena** e **Lílian** pela amizade e apoio.

- Aos meus amigos de todas as horas: **Juliana** e **Augusto**, **Daniele**, **Renata** e **Greco**, **Bruno** e **Cristina**, **Fabiana**, **Clarisse** e **Luis César**, pelo apoio e compreensão das muitas horas ausentes.

- Aos meus pais, **Walter** e **Eliana**, por todo o amor e incentivo que sempre me deram em toda a minha vida e me que tornaram a pessoa que eu sou hoje; à minha irmã **Patricia** e ao meu cunhado **Henrique** por todo o apoio e carinho e por me darem de presente o ser mais amado deste mundo, meu sobrinho e minha vida Guilherme; às minhas tias queridas **Tadéa** e **Dora** por estarem sempre presentes na minha vida; a todos os meus tios, tias, primos e primas que de uma forma ou de outra colaboraram para a realização de mais esta etapa e que fazem parte da minha tão amada família.

## ORAÇÃO DE SÃO FRANCISCO DE ASSIS

Senhor fazei de mim o instrumento de Vossa paz
Onde houver ódio, que eu leve o amor
Onde houver ofenças, que eu leve o perdão
Onde houver discórdia, que eu leve a união
Onde houver trévas, que eu leve a luz
Onde houver erro, que eu leve a verdade
Onde houver desespero, que eu leve a espença
Onde houver tristeza, que eu leve alegria
Onde houver dúvidas, que eu leve a fé
Ó Mestre, fazei que eu procure mais
Consolar que ser consolado
Compreender que ser compreendido
Amar que ser amado
Pois é dando que se recebe
É perdoando que se é perdoado
E é morrendo que se vive para vida eterna.

Resumo da Dissertação apresentada à COPPE/UFRJ como parte dos requisitos necessários para a obtenção do grau de Mestre em Ciências (M.Sc.)

# CONFIABILIDADE DE SISTEMAS INSTRUMENTADOS DE SEGURANÇA: ANÁLISE CUSTO-BENEFÍCIO DE ALTERNATIVAS PARA O ATENDIMENTO AO SIL REQUERIDO EM INSTALAÇÕES INDUSTRIAIS

Luciana Moreira Chame

Maio/2007

Orientadores: Basílio de Bragança Pereira
Paulo Fernando Ferreira Frutuoso e Melo

Programa: Engenharia de Produção

As Normas internacionais IEC 61508/61511 indicam vários métodos para a determinação do SIL requerido para uma função instrumentada de segurança. Após a determinação do SIL requerido, resta o problema da implementação prática deste requisito. Neste trabalho é feita uma análise comparativa das alternativas que podem ser utilizadas para o atendimento ao SIL requerido e das suas implicações em relação ao custo do ciclo de vida das instalações. O atendimento a níveis de SIL mais elevados requer uma avaliação detalhada das alternativas, que variam desde a utilização de componentes mais confiáveis à utilização de configurações alternativas de redundância ou diferentes políticas de testes, incluindo a possibilidade de realização de testes parciais. O trabalho apresenta ainda os principais métodos para a avaliação da PFD, com a inclusão de testes parciais e falhas de causa comum, fazendo sua aplicação ao caso prático da função de proteção contra alta pressão (HIPPS) em uma planta petroquímica. A análise dessas alternativas mostrou que a adoção inteligente de testes parciais com freqüências mais altas, combinada com a realização de testes completos com freqüências mais baixas, é capaz de garantir o atendimento ao SIL 3 e ainda ser custo-eficiente, em casos onde paradas completas do processo apresentem altos custos.

Abstract of Dissertation presented to COPPE/UFRJ as a partial fulfillment of the requirements for the degree of Master of Science (M.Sc.)

SAFETY INSTRUMENTED SYSTEMS RELIABILITY: COST-BENEFIT ANALYSIS OF ALTERNATIVES FOR COMPLIANCE WITH REQUIRED SIL IN INDUSTRIAL UNITS

Luciana Moreira Chame

May/2007

Advisors: Basílio de Bragança Pereira
Paulo Fernando Ferreira Frutuoso e Melo

Department: Industrial Engineering

IEC 61508/61511 standards clearly indicate several methods for the determination of the required SIL for a Safety Instrumented Function. After determining the required SIL there remains the problem of its practical implementation. This work proposes a comparative analysis of alternative ways that can be used to comply with the required SIL and their implications with respect to the lifecycle cost of the protected installations. Compliance with high required safety integrity levels requires a detailed evaluation of the alternatives which vary from the utilization of more reliable components to configurations with higher redundancy or the use of more frequent testing policies. The latter may also include the possibility of using partial-stroke testing. This work also presents the main methods for evaluating the PFD for partial-stroke testing schemes, and its application to a real case of a HIPPS function in a petrochemical plant. The comparative analysis of those alternatives has shown that the intelligent use of partial-stroke tests with higher frequencies combined with the performance of complete tests with lower frequencies is capable of guaranteeing compliance with SIL-3 and still be cost-efficient in cases where shutdowns of the process for complete tests of the SIF represent high costs.

# Sumário

# Lista de Figuras

# Lista de Tabelas

# Capítulo 1

# Introdução

A busca por soluções otimizadas apresenta um dos maiores desafios para todas as áreas de atividade produtiva relacionadas à ciência e tecnologia, principalmente para os diversos setores industriais inseridos em um ambiente extremamente competitivo, onde a pressão para orientar seus esforços no intuito de conseguir o máximo rendimento e desempenho, associado a menores custos, se faz cada vez mais presente e necessário. No entanto, a procura por esta solução ótima é função de variáveis um pouco antagônicas, dado que a melhoria do processo produtivo está cada vez mais baseada em sistemas complexos e sofisticados, e ao mesmo tempo, limitado por restrições financeiras e requisitos de segurança. Dado este contexto, diversas técnicas de otimização do desempenho de sistemas têm sido cada vez mais discutidas e estudadas, buscando lidar com estas e outras variáveis, de forma a se conseguir a melhor relação entre custos, segurança e desempenho dos processos produtivos.

Toda atividade indutrial está associada a um perigo no seu uso ou emprego, onde as conseqüências de um acidente são indesejáveis. Nenhum processo produtivo está livre da ocorrência de falhas, sendo estes eventos intrínsecos ao sistema. As falhas, embora não possam ser totalmente evitadas, podem ser toleradas até um determinado nível que não inviabilize a operação, nem pelo da segurança, nem pelo econômico. Para avaliar estes sistemas, uma ferramenta científica, com base na lógica e na probabilidade, chamada de Análise de Confiabilidade de Sistemas, se tornou um importante meio pelo qual podem se obter melhorias operacionais e aumento de segurança. O conceito desta técnica está ligado ao sucesso da operação do sistema, por um determinado período de

tempo e de condições de operação específicas.

A confiabilidade pode, portanto, ser entendida como um aspecto de incerteza de engenharia, e de acordo com o sistema ou com o objetivo específico do usuário do sistema, o estudo de confiabilidade é voltado para a obtenção de uma aplicação particular. Esta aplicação é traduzida como atributos de interesse para o sistema em questão. A engenharia de confiabilidade tornou-se uma das técnicas que possibilita a otimização dos processos produtivos, tendo também, como objetivo, a identificação e prevenção de acidentes passíveis de ocorrer em uma instalação industrial.

Todo o equipamento ou sistema, mesmo o mais sofisticado, pode falhar. Falhas em equipamentos ou sistemas em uma planta podem resultar em danos ao meio ambiente, explosões, ferimentos e morte de pessoas. O conceito de SIL (Nível de Integridade de Segurança, ou do inglês: *Safety Integrity Level*) considera as falhas e suas conseqüencias, além de ser um enfoque reconhecido mundialmente para instalações de segurança. Além disso, o conceito de SIL permite ao operador da planta definir as exigências para seu equipamento dependendo dos danos esperados, bem como fornece ao fabricante do produto um modo de descrever o comportamento de falha do mesmo (por exemplo, em termos de aceitabilidade).

## 1.1 Motivação

Durante os últimos anos, grandes acidentes como Flixborough, Bhopal, Chernobyl e Piper Alpha têm acarretado um grande número de vítimas e aumentado a percepção pública dos riscos associados com a operação de grandes plantas de processo. Depois de tais acidentes, a reação é sempre "isto não deve acontecer novamente"; entretanto, é visivelmente impossível eliminar todos os riscos. Para o público em geral e os órgãos governamentais reguladores na sociedade moderna, há então a necessidade de comprometimento para resolver o aparente paradoxo de se obter os benefícios da tecnologia moderna sem incorrer nos problemas que esta mesma tecnologia pode trazer (ANDREWS & MOSS 2002).

Na medida em que os acidentes industriais ocorrem, intensifica-se a implementação de medidas de proteção para se tentar evitá-los. Este movimento tem seguido uma trajetória ascendente ao longo das últimas décadas, enfatizando cada vez mais a im-

portância de se garantir a confiabilidade dos sistemas de proteção das unidades de produção industrial. A introdução dos chamados Sistemas Instrumentados de Segurança (SIS) facilitou sobremaneira a utilização em larga escala de sistemas de intertravamento cada vez mais complexos e sofisticados, entretanto, trouxe uma série de questionamentos sobre os níveis de confiabilidade requeridos e alcançados por tais sistemas. Em parte como resposta a esses questionamentos, foram publicadas as normas internacionais IEC 61508 (IEC-61508 1998) e IEC 61511 (IEC-61511 2003), que estabelecem os critérios para o desenvolvimento e a aplicação de SIS, respectivamente, na indústria em geral e em plantas petroquímicas em particular. Adotando um enfoque de ciclo de vida (do projeto ao descomissionamento), os critérios giram em torno dos chamados níveis de integridade de segurança, comumente denominados SIL.

Os sistemas tecnicamente complexos, como aviões, reatores nucleares, refinarias e plantas químicas não podem mais ser construídos baseados na intuição ou experiência empírica. Os riscos envolvidos em grandes sistemas técnicos modernos são simplesmente muito grandes para se aprender por tentativa e erro. Decisões deste tipo precisam envolver análises técnicas bem fundadas e julgamento baseado em boas práticas de engenharia (GRUHN & FINKEL 2002).

Conforme citado, os chamados sistemas instrumentados de segurança (ou sistemas de *shudown*) para processos industriais têm evoluido bastante nestas últimas décadas, em termos de concepção, projeto e implementação. A evolução não é fruto do acaso, nem apenas do desenvolvimento de uma consciência de que os acidentes podem e devem ser evitados. Infelizmente, é a partir da análise de acidentes realmente ocorridos que se tomou conhecimento de que os sistemas de segurança normalmente empregados em instalações industriais deixavam muito a desejar (BEGA, DELMÉE, COHN, BULGARELLI, KOCH & FINKEL 2003). Os sistemas eletrônicos de proteção configuram-se como um dos elementos mais importantes para a garantia da integridade física de instalações industriais e para a segurança daqueles que nelas trabalham (GAMAL 1993).

Selecionar e projetar um sistema de segurança não é uma tarefa trivial e nunca será. Uma das razões para isso é o desafio de atender a padrões internacionais conciliando conceitos como segurança e disponibilidade, conceitos estes cruciais para atender à demanda por maiores campanhas de produção, maiores intervalos entre testes, menores tempos de parada, maior necessidade de atingir metas de produção, entre outros.

Muitos projetos de redução de risco são financeiramente inviáveis por proporem um nível de redução de riscos desproporcional ao seu custo. Desta forma os projetistas devem balancear o quanto de risco se quer reduzir com um determinado sistema de segurança com o custo do ciclo de vida do sistema que será instalado. Bons projetos irão otimizar o custo do ciclo de vida, garantindo entretanto, o nível de segurança requerido pelo sistema.

Atributos de confiabilidade devidamente quantificados permitem fazer uma análise comparativa entre várias configurações alternativas, podendo com isso dizer que um determinado projeto é melhor ou pior do que outro em termos de confiabilidade. Portanto, a análise de confiabilidade pode ser entendida como um meio essencial de avaliar quantitativamente a operação e a segurança de sistemas, na qual sua aplicação depende de um acompanhamento do funcionamento real do sistema, aliado ao desenvolvimento de uma metodologia científica aplicada.

Desta forma, é possível dizer que na elaboração do um projeto de sistema de um segurança para plantas industriais, torna-se de fundamental importância a combinação da análise de confiabilidade e do custo do ciclo de vida (CCV) como critério decisório na avaliação de alternativas de projeto. O critério tem como premissa básica para a tomada de decisão a avaliação do desempenho do sistema de segurança e o valor do CCV, sendo que a primeira avaliação tem prioridade sobre a segunda, ou seja, primeiramente é exigido que o sistema de segurança garanta o atendimento a um certo nível de segurança e em seguida, busca-se dentre as alternativas de projeto, aquela que proporcione o menor custo do ciclo de vida (CCV). A combinação de análise de confiabilidade e custo do ciclo de vida na escolha de alternativas de projetos torna-se um poderoso instrumento decisório na engenharia.

## 1.2 Objetivos do Trabalho

A utilização de técnicas de análise de confiabilidade permite que os níveis de confiabilidade de várias configurações alternativas para o projeto de um determinado sistema de proteção sejam avaliados quantitativamente. Os índices quantitativos obtidos na análise constituem-se em elementos importantes para o projetista, possibilitando o conhecimento das variações relativas à confiabilidade entre as diferentes configurações

e para a identificação dos componentes do sistema que mais contribuem para a sua probabilidade de falha. No entanto, na grande maioria das vezes, a variação relativa dos índices de confiabilidade não se constitui em argumento suficiente para a tomada de decisão relativa à escolha de uma das alternativas consideradas. Portanto, de modo geral, o processo de tomada de decisão requer a realização de um balanço entre os custos de cada configuração e os seus benefícios associados. A realização deste balanço é o fundamento básico de uma Análise Custo-Benefício.

Neste trabalho propõe-se a aplicação de técnicas de análise de confiabilidade e de análise do custo do ciclo de vida, de forma integrada, com o objetivo de tomada de decisão para a escolha de alternativas que apresentem as melhores relações custo-benefício e atendam a um determinado requisito de confiabilidade mínimo pré-estabelecido. Desta forma, é possível dizer que o objetivo principal deste trabalho consiste em, através de uma análise do custo do ciclo de vida, fornecer subsídios para a formulação da estratégia de implementação de um nível de confiabilidade requerido para um sistema de segurança de uma instalação industrial.

O estudo de caso analisado para a aplicação da metodologia proposta, consiste em fornecer subsídios para a formulação da estratégia de implementação a ser adotada pelos responsáveis pelo projeto de um determinado sistema de segurança de uma empresa do ramo petroquímico, de um sistema de bloqueio para proteção do *header* do flare de uma grande planta petroquímica. Para tanto, é feita uma análise comparativa de alternativas que podem ser utilizadas para o atendimento de um determinado nível de SIL requerido e das suas implicações em relação ao custo do ciclo de vida das instalações. Por exemplo, em se tratando do atendimento a um nível SIL 1, o problema pode ser facilmente resolvido utilizando-se uma simples configuração 1-1-1 (iniciador-lógica-atuador) e uma freqüência de testes que não causa muito impacto na operação. No entanto, o atendimento a níveis de SIL mais altos, como SIL 3 (requisito desta avaliação), requer um estudo mais detalhado das várias alternativas disponíveis, as quais variam desde a utilização de componentes mais confiáveis (com certificados de atendimento, por exemplo) ao emprego de configurações com diferentes níveis de redundância ou diferentes políticas de testes das Funções Instrumentadas de Segurança (FIS), incluindo a possibilidade de realização de testes parciais do sistema ("partial stroke testing").

As normas internacionais IEC 61508/61511 indicam vários métodos para a determinação do SIL requerido para uma função instrumentada de segurança (FIS). Após a determinação deste SIL requerido, resta o problema da implementação prática deste requisito. O primeiro passo para esta "implementação prática deste requisito" é o cálculo do valor do atributo de confiabilidade PFD (Probabilidade de Falha na Demanda) e a posterior análise das possíveis alternativas para adequação deste valor ao valor de confiabilidade requerido pelo sistema. No caso do presente estudo, esta avaliação de confiabilidade é embasada com a conseqüente determinação do custo do ciclo de vida de cada uma das dez alterntativas propostas para o SIS em questão.

A Norma IEC 61508 (IEC-61508-6 2000), além de indicar os métodos para a avaliação do SIL Requerido, fornece também várias equações para a avaliação quantitativa da PFD de várias configurações de sistemas de segurança. No entanto, a norma não apresenta as correspondentes deduções das expressões apresentadas, nem sequer explicita as premissas e aproximações usadas para se chegar às equações para cada uma das configurações de SIS. Desta forma, além do objetivo principal citado anteriormente, outros objetivos deste trabalho estão relacionados a seguir:

- Apresentar as deduções formais das equações das PFDs das várias configurações apresentadas na Parte 6 da Norma IEC 61508, evidenciando de forma clara, as principais premissas e aproximações embutidas nas mesmas;

- Apresentar a equação para a avaliação da PFD para uma configuração *koon* qualquer e sua correspondente dedução, as quais não são apresentadas nas normas;

- Mostrar os resultados quantitativos para alguns sistemas típicos usados na indústria de processos e comentar as limitações impostas pelas chamadas falhas de causa comum sobre as PFDs dos sistemas;

- Discutir os efeitos práticos das restrições de arquitetura dos sistemas de segurança impostas na Norma IEC 61508 sobre os níveis de SIL capazes de serem alcançados por algumas configurações;

- Analisar diversas arquiteturas de SIS e sua adequação ao nível de redução de risco pretendido;

- Propor períodos de testes adequados à instrumentação escolhida ou disponível, em função de critérios técnicos e econômicos.

Portanto, pode-se dizer que este trabalho visa esclarecer alguns conceitos básicos que estão por trás das expressões apresentadas na Norma IEC 61508, generalizando-as para outras configurações, bem como fornecer alguns exemplos práticos ilustrando os seus usos e os efeitos práticos das restrições impostas pela norma para se alcançar o nível de SIL Requerido com algumas configurações.

Neste trabalho, a análise comparativa é feita para o caso prático de um SIS para proteção contra alta pressão em uma torre de uma planta petroquímica, ou HIPPS, do inglês "High Integrity Pressure Protection Systems". A análise comparativa realizada mostrou que a adoção inteligente de testes parciais com uma freqüência mais alta, combinada com a realização de testes completos com uma freqüência mais baixa (até de 1 a cada 5 anos), pode ser capaz de garantir o atendimento ao SIL 3 requerido, sendo custo-eficiente, em casos onde uma parada completa do processo para a realização do teste total tenha um alto custo, caso que ocorre na maioria das plantas petroquímicas.

## 1.3 Apresentação do Estudo de Caso Analisado

Uma das questões mais importantes para a segurança de plantas de processos é a prevenção de eventos de perda de contenção causados por pressão excessivamente alta. Um acidente com perda de contenção por alta pressão pode ter graves conseqüências para os trabalhadores, o meio ambiente e para o patrimônio da empresa, devido à possibilidade de ocorrência de uma grande liberação de produtos tóxicos ou inflamáveis. Para se evitar esse tipo de problema, é fato conhecido dos projetistas dessas plantas que todos os vasos de pressão, devem ser dotados de sistemas de alívio para a proteção dos mesmos contra eventuais episódios de alta pressão.

Na realização de um projeto de expansão de uma grande planta petroquímica, à qual seriam adicionadas duas novas unidades de processo, foi verificado que o *header* do flare não teria capacidade para receber a descarga resultante da despressurização conjunta das unidades novas e existentes em caso de um desligamento súbito de todas as unidades da instalação. Neste caso, a solução tradicional obrigaria à ampliação do *header* atual

ou à construção de um novo *header* para atender à demanda das unidades novas. Ambas as soluções envolvem altos custos e causariam sérios transtornos operacionais.

Em linha com as novas possibilidades abertas pelas atuais normas de projeto, os responsáveis pelo projeto buscaram a solução do problema através da utilização de um Sistema HIPPS, do inglês "High Integrity Pressure Protection Systems". Neste caso, a função do HIPPS seria a de bloquear a fonte de energia (vapor) para o refervedor da torre principal de uma das novas unidades no momento de um desligamento súbito conjunto de todas as unidades da instalação.

Uma análise de risco foi conduzida para a determinação do nível de confiabilidade requerido para o novo Sistema de Bloqueio do Refervedor, a qual investigou todos os cenários de acidente que levariam à despressurização da torre para o flare e concluiu pela necessidade de atendimento a um alto nível de confiabilidade, ou ainda, a um baixo valor de probabilidade de falha na demanda, no caso dos eventos de despressurização conjunta de todas as unidades (tais como perda de energia elétrica ou falhas de outras utilidades comuns).

O problema analisado neste estudo consiste exatamente na seleção de uma alternativa de configuração para o sistema de segurança, de modo que o mesmo atenda ao requisito pré-determinado de confiabilidade e apresente a melhor relação custo-benefício para o investidor. A minimização dos custos globais de um projeto nem sempre é uma tarefa fácil. Desta forma, a correta escolha de todos os componentes deste sistema de segurança apresenta-se como uma oportunidade para a redução nos custos globais da instalação, ao longo da sua vida útil. A avaliação dos custos do sistema ao longo da sua vida útil pode ser realizada por várias metodologias, sendo aqui proposta a análise pelo estudo do Custo do Ciclo de Vida do sistema (análise conjunta de engenharia/economia e período de retorno do investimento).

## 1.4 A Organização do Trabalho

Esta dissertação encontra-se dividida em sete capítulos, conforme descrito a seguir.

O Capítulo 2 aborda conceitos e definições que serão utilizados ao longo da dissertação e que consistem de informações fundamentais para o completo entendimento do trabalho desenvolvido, como os conceitos de análise custo-benefício e os conceitos

básicos de confiabilidade, incluindo tópicos sobre falhas de componentes, função densidade de probabilidade e função de confiabilidade.

O Capítulo 3 apresenta os conceitos de sistemas instrumentados de segurança (SIS), discutindo tópicos como funções instrumentadas de segurança (FIS), probabilidade de falha na demanda (PFD) e nível de integridade de segurança (SIL). As principais Normas e Referências Metodológicas relacionadas ao tema deste trabalho também são apresentados neste capítulo, bem como os conceitos de ciclo de vida de segurança. Da mesma forma, também são apresentadas as Restrições de Arquitetura de *Hardware* dos sistemas de segurança quanto ao máximo nível de integridade (SIL) atingível por uma malha de segurança em função das características dos seus componentes, de acordo com a Norma IEC 61508.

O Capítulo 4 descreve resumidamente as principais metodologias disponíveis na literatura para a determinação do SIL requerido, apresentando metodologias qualitativas e semi-qualitativas para a avaliação do nível de confiabilidade requerido pelos sistemas de segurança.

O Capítulo 5 tem como objetivo discutir as diferentes alternativas para o cálculo da Probabilidade de Falha na Demanda (PFD) de Funções Instrumentadas de Segurança (FIS) e apresentar detalhadamente a técnica sugerida pela Parte 6 da Norma do IEC 61508, incluindo a apresentação da metodologia proposta, a dedução das equações de cálculo, inclusive para uma configuração *koon* qualquer, bem como discutir a possibilidade de testes parciais de componentes do sistema de segurança analisado, o fator de diagnóstico de cobertura, a modelagem das falhas de causa comum e de testes imperfeitos.

O Capítulo 6 apresenta um estudo de caso que consiste em uma análise custo-benefício, utilizando como ferramenta uma análise do custo do ciclo de vida de diferentes alternativas para um sistema de segurança, buscando identificar a melhor configuração de sistema de bloqueio rápido de entrada de vapor para um refervedor de uma torre de uma unidade petroquímica, de forma a impedir a pressurização excessiva e conseqüente despressurização para o flare, através da válvula de alívio, em caso de um desligamento súbito conjunto de todas as unidades da instalação, de modo que o mesmo atenda ao requisito de SIL 3.

Finalmente, o Capítulo 7 apresenta as conclusões e contribuições deste trabalho e

sugere novas direções para a continuação desta linha de pesquisa.

O Apêndice A apresenta o cálculo da probabilidade de falha na demanda para as arquiteturas mais usuais, usando a Norma IEC 61508 e as fómulas deduzidas e apresentadas no Capítulo 5 deste trabalho.

# Capítulo 2

# Conceitos Fundamentais

## 2.1 Introdução

Este capítulo tem como intuito apresentar alguns conceitos e definições que serão utilizados ao longo da dissertação e que consistem de informações fundamentais para o completo entendimento do trabalho desenvolvido. A primeira seção discute brevemente o conceito de uma análise custo-benefício e a seção seguinte, apresenta conceitos básicos de confiabilidade, abordando conceitos de falhas, de função de confiabilidade e função densidade de probabilidade, fundamentais para o entendimento da avaliação que é feita nos capítulos subseqüentes.

## 2.2 Análise Custo-Benefício

De forma simplificada, uma análise custo-benefício consiste no levantamento dos custos e benefícios resultantes de se estudar determinadas alternativas, como por exemplo, resultantes da implementação de uma dada configuração num sistema de segurança. Conforme GAMAL (1993), o balanço econômico destes custos e benefícios indicará se a mesma é recomendável ou não: se positivo, indica que haverá um ganho líquido (lucro) e, portanto, a configuração é recomendável, caso contrário, outra solução deverá ser proposta. Aplicando este processo a várias configurações, pode-se escolher aquelas que apresentarem as melhores relações de custo e benefício.

Neste trabalho serão analisadas e avaliadas diferentes alternativas de um sistema

de segurança, visando obter a melhor alternativa custo-benefício para o investidor, dado a obrigatoriedade de atender a requisitos pré-estabelecidos. Os custos associados às configurações são basicamente relacionados à implementação dos equipamentos e à manutenção destes. Por sua vez, o benefício resultante da implementação de uma configuração apropriada é obtido levando-se em consideração: a redução das perdas esperadas devido a acidentes (benefício resultante da atuação do sistema de proteção, evitando o acidente e avaliado em função da sua probabilidade de falha na demanda), a redução das perdas esperadas devido a falhas espúrias (redução da freqüência de falhas espúrias que levem a parada desnecessária da unidade), bem como a minimização de despesas com a manutenção e operação dos sistemas avaliados.

### 2.2.1 A Análise Custo-Benefício e o Custo do Ciclo de Vida

A minimização dos custos globais de um projeto nem sempre é uma tarefa fácil. Conforme citado, a análise proposta neste trabalho é a seleção de uma alternativa de configuração de um sistema de segurança que, em função de medidas pré-estabelecidas de sucesso do sistema, apresente a melhor relação custo-benefício para o investidor. Desta forma, a correta escolha de todos os componentes deste sistema de segurança apresenta-se como uma oportunidade para redução nos custos globais da instalação, ao longo da sua vida útil. A avaliação dos custos do sistema ao longo da sua vida útil, pode ser realizado por várias metodologias, sendo aqui proposta a análise pelo estudo do Custo do Ciclo de Vida do sistema (análise conjunta de engenharia/economia e período de retorno do investimento).

Muitos sistemas são concebidos considerando apenas o investimento inicial, originando sistemas que apresentam grandes custos de manutenção e operação. A crescente competitividade dos mercados nacionais e internacionais obriga a um esforço contínuo de modo a aumentar a competitividade, fazendo com que as empresas procurem soluções que visem a redução dos custos globais e o aumento dos rendimentos operacionais. A operação/manutenção, principalmente no setor de sistemas de segurança de instalações industriais, continua a merecer uma atenção particular como fonte de poupança de custos, especialmente devido à minimização dos custos decorrentes de tempos de parada da produção.

O Custo do Ciclo de Vida (CCV) pode ser entendido como uma ferramenta de gestão que visa ajudar a minimização de custos e a maximização do rendimento para variados tipos de sistemas. A determinação do CCV é um método que permite a comparação de soluções alternativas, em termos de custos, sendo basicamente um processo matemático, mas extremamente dependente da informação disponível, logo, os resultados do processo apresentam certamente um grau de confiança similar ao dos dados utilizados.

O CCV de qualquer sistema é o custo total durante o seu período de vida útil, no entanto, os fatores de custo que devem ser consideradas em uma análise do custo do ciclo de vida varia de sistema para sistema. Por exemplo, de forma geral, é possível dizer que estes fatores representam os custos de aquisição, instalação, operação, manutenção (preventiva e corretiva), paradas, ambientais e de desmontagem do equipamento. A identificação de todas as parcelas envolvidas apresenta-se como uma etapa fundamental nesta metodologia. Quando o CCV é utilizado como uma ferramenta de comparação entre diferentes alternativas, o processo de cálculo do CCV indicará, de forma isenta, a solução que apresenta menor custo global, com base nas informações disponíveis. As parcelas envolvidas no cálculo do CCV das alternativas propostas neste trabalho serão detalhadas na seção 6.7.2.

Uma análise de risco e/ou de confiabilidade irá fornecer uma ou mais medidas de sucesso ou falha do sistema, conforme é o caso neste trabalho. Nas próximas seções deste capítulo, serão apresentados conceitos fundamentais de confiabilidade e de medidas de sucesso e falha de um sistema instrumentado de segurança, que são fundamentais para o entendimento da abordagem utilizada para o cálculo do custo do ciclo de vida e, conseqüentemente da análise custo-benefício realizada.

## 2.3 Conceitos Básicos de Confiabilidade

### 2.3.1 Introdução à Confiabilidade

Conforme cita LAFRAIA (n.d.), se alguém lhe perguntasse quais são as características desejáveis em um produto, certamente você responderia que ele deveria ter uma vida ilimitada e que durante esta vida ele deveria funcionar isento de falhas, porém

isso dificilmente será algum dia alcançado.

Na sociedade moderna em que vivemos, cada avanço no campo tecnológico representa uma melhoria na qualidade de vida do ser humano, melhoria esta, que pode ser observada também através da confiabilidade de um determinado produto ou serviço, pelo qual estamos usufruindo. De fato, no cotidiano do ser humano, o conceito de confiabilidade está intimamente presente, pois a idéia de um produto ou serviço seguro, durável, imune a falhas, disponível, rápido, ou seja, confiável, torna-se cada vez mais corriqueiro, manifestando-se como uma das maneiras pela qual pode-se verificar a qualidade deste produto ou serviço (DINIZ 1997).

Pode-se dizer que a necessidade de uma avaliação do nível de segurança de sistemas teve um grande impulso com o desenvolvimento de certas indústrias, principalmente a aeronáutica e a nuclear. Devido ao perigo envolvido nestas atividades, grandes esforços foram feitos no sentido de se ter sistemos projetados com o conhecimento prévio do seu grau de segurança.

No início do século XX, utilizava-se de fatores de segurança excessivamente altos para tentar minimizar os problemas de confiabilidade dos equipamentos. Tratava-se da adoção de uma filosofia do tipo "projetar-testar-reprojetar" ou também referida como "voe-conserte-voe", pela indústria aeronáutica. A partir da década de 30 do século passado, a aplicação deste enfoque foi se tornando impraticável, devido basicamente a dois fatores: o grande aumento da velocidade de desenvolvimento de novos projetos e o desenvolvimento de equipamentos cada vez mais complexos e caros. Gradativamente, o enfoque intuitivo foi cedendo lugar a um novo enfoque, pelo qual, a confiabilidade do equipamento passou a ser estatisticamente definida e calculada, tornando-se parte fundamental do projeto do equipamento, desde a sua concepção inicial.

A confiabilidade é, portanto, um aspecto de incerteza de engenharia. Se um item vai trabalhar durante um certo período de tempo, é uma questão que pode ser respondida com uma probabilidade (LAFRAIA n.d.). Ou seja, matematicamente, a confiabilidade pode ser definida como a probabilidade de que um componente ou sistema cumpra sua função com sucesso, por um período de tempo previsto, sob condições de operação especificadas.

É possível ressaltar quatro aspectos relacionados com a definição de confiabilidade, representada normalmente por R (do inglês, *Reliability*) (OLIVEIRA & FLEMING

1997):

- Natureza probabilística (o valor da confiabilidade pode variar de 0 a 1);
- Dependência temporal (a confiabilidade depende do tempo de missão);
- Critério de sucesso (a confiabilidade depende da especificação do desempenho desejado); e
- Condições de operação (dependendo das condições a confiabilidade pode variar significativamente).

De acordo com o sistema ou com o objetivo específico do usuário do sistema, o estudo de confiabilidade é voltado para obtenção de uma aplicação particular. Esta aplicação é traduzida como atributos de interesse para o sistema em questão. Exemplos de atributos de confiabilidade considerados numa análise quantitativa podem ser: o tempo médio até falhar, a confiabilidade, a disponibilidade e a manutenabilidade, entre outros. Para este trabalho em particular, o atributo de confiabilidade apropriado é a probabilidade de falha na demanda, atributo este que será discutido, na seção 3.3.

A troca de equipamentos e a substituição de sistemas ou processos manufaturados por processos automatizados está instintivamente associada à condição de aumento da confiabilidade do processo produtivo. De fato, esta se apresenta como uma das condicionantes para o aumento da confiabilidade no processo e conseqüentemente da diminuição dos custos relativos a perdas e paradas de produção (LIMA 2002).

### 2.3.2 Falhas de Componentes

Conforme discutido na seção anterior, o conceito de confiabilidade está diretamente relacionado ao de falha. Desta forma, esta seção apresenta conceitos e discute importantes aspectos de falhas, abordando pontos como taxas de falha, modos de falha, tipos de falha e falhas de causa comum.

OLIVEIRA (1985) define uma falha como o término da habilidade de um componente em cumprir sua função. Da mesma forma, um estado de falha foi definido como aquele em que o equipamento não desempenha mais sua função de acordo com os padrões mínimos aceitáveis. A falha não se refere ao equipamento como um todo,

mas sim às funções que ele se propõe a desempenhar. Deste modo, defeito e falha têm o mesmo significado, desde que determinada função de um equipamento não seja desempenhada ao mínimo necessário e estabelecido.

Dentro do universo de falhas, é possível classificá-las quanto à:

- Dependência em relação a falhas de outros componentes;
- Visibilidade da falha no momento em que ocorre;
- Relevância do momento em que a falha é revelada; e
- Suas conseqüências.

Desta forma, temos que:

(A) Classificação de Falhas quanto à dependência em relação a falhas de outros componentes:

- Falha Independente: aquela cuja probabilidade de ocorrência é estatísticamente independente da probabilidade de ocorrência de falhas de outros componentes.
- Falha Dependente: duas falhas são chamadas dependentes quando a probabilidade de ocorrência de uma delas guarda algum tipo de dependência estatística com a probabilidade de ocorrência da outra.

(B) Classificação de Falhas quanto à visibilidade da falha no momento em que ocorre:

- Falha Revelada ou Evidente ou Anunciada: aquela que é revelada (vista, sentida ou detectada) para o operador/operação no momento em que ocorre.
- Falha Oculta: aquela que não é revelada (vista, sentida ou detectada) pelo operador/operação no momento em que ocorre, permanecendo oculta até a ocorrência de algum evento posterior que a revele (tipicamente uma demanda ou um teste).

(C) Classificação de Falhas quanto à relevância do momento em que a falha é revelada:

- Falha Operacional ou em Funcionamento: aquela que ocorre durante o período de funcionamento do equipamento.
- Falha na Demanda: aquela que ocorre durante o período de reserva do equipamento e que é revelada no momento em que este é demandado.

(D) Classificação de Falhas quanto às suas conseqüências:

- Falha Perigosa ("Dangerous failure"): falha que tem o potencial de levar o sistema para um estado perigoso ou falho em desempenhar sua função, ou ainda, falha que faz com que o sistema não opere na demanda.
- Falha Segura ("Safe failure"): falha que não tem o potencial de levar o sistema para um estado perigoso ou falho em desempenhar sua função, ou ainda, falha que faz com que o sistema opere sem que uma demanda tenha ocorrido.

Conforme apresentado então, dentro do universo de falhas que podem ocorrer, existem as falhas dependentes e as independentes. As falhas independentes são aquelas que provocam falhas de um único componente, sem qualquer relação com outros componentes. Métodos têm sido utilizados em sistemas no sentido de minimizar o impacto de falhas simples de equipamentos usando o princípio de redundância. Por outro lado, as falhas dependentes podem ser definidas como aquelas surgidas de uma causa que provoca a falha simultânea de mais de um dentre os componentes do sistema. As falhas dependentes são causadas normalmente por erros de manutenção ou influência do meio ambiente (umidade, altas temperaturas, etc.) Este tipo de falha tem um importante espaço no estudo de confiabilidade, dado que ele reduz a confiabilidade de sistemas que contêm componentes redundantes. Estas falhas dependentes, denominadas "falhas de causa comum" deste ponto em diante, abreviadas por FCC, serão discutidas mais detalhadamente, na seção 2.3.2.2.

#### 2.3.2.1 Taxa de Falha e Modo de Falha

O conhecimento do processo de falha é muito útil no estudo de confiabilidade, uma vez que existem vários valores de taxas de falha de um componente disponíveis

na literatura especializada. Cada valor deste, depende do modo pelo qual a falha se manifesta, isto é, seu modo de falha. Portanto, os diferentes modos de falha de um componente são as diferentes maneiras pelas quais as falhas dos componentes se manifestam.

Modo de Falha pode ser entendido como maneiras pelas quais um componente pode falhar, ou seja, o conjunto de efeitos pelos quais uma falha é observada. Por exemplo, considerando um determinado equipamento, pelo menos dois tipos de modos de falha podem ser destacados: a falha na partida, ou seja, o equipamento ou não consegue iniciar seu funcionamento, ou dá a partida e logo após um período de tempo falha; ou falha em operação, ou seja, o componente deixa de obedecer aos critérios de sucesso estabelecidos após entrar em funcionamento.

Outro importante conceito é o da Taxa de falha, normalmente expresso pelo termo $\lambda$, e que pode ser descrito como uma função tal que $\lambda(t)dt$ fornece a probabilidade de que um item (componente) que não falhou entre 0 e $t$, sofra uma falha entre $t$ e $t + dt$, ou ainda, conforme OLIVEIRA (2006), $\lambda(t)dt$ é a probabilidade de que um componente que funcione em $t$ falhe entre $t + dt$ e a taxa de falha em $t$, $\lambda(t)$, é o limite desta probabilidade dividida por $dt$, quando $dt$ tende a zero.

Taxas de falhas e modos de falha fornecem ao usuário um entendimento de como o dispositivo se comporta no estado manufaturado e são encontrados em grande diversidade de literatura como por exemplo, OREDA - *Offshore Reliability Data* (OREDA 2002) e SINTEF (HAUGE, LANGSETH & ONSHUS 2006), já disponíveis aos usuários, chamados de banco de dados. Estes bancos de dados contêm uma lista de componentes e equipamentos que operam em condições específicas de trabalho. Estes dados também podem ser obtidos através de consulta aos fabricantes ou deduzidos a partir de coleta e análise de dados operacionais.

#### 2.3.2.2 Falha de Causa Comum

Sistemas de segurança normalmente utilizam redundâncias, incorporadas para prover uma alta probabilidade de sucesso dos mesmos. Quando quantificada a probabilidade de sucesso, os subsistemas redundantes não irão sempre falhar independentemente. Um simples modo de falha comum pode afetar componentes redundantes num mesmo momento. Em estudos de segurança, os cálculos devem também levar em conta estas

falhas de causa comum, ou FCC (ANDREWS & MOSS 2002).

Apesar de não haver uma única e universal definição para falhas de causa comum, uma conceituação bastante aceita é fornecida por (MOSLEH, RASMUSON & MARSHALL 1998): "Falhas de Causa Comum são um subconjunto de falhas dependentes em que dois ou mais estados falhos de componentes existem ao mesmo tempo, ou em um curto intervalo de tempo, e são o resultado direto de uma causa em comum (compartilhada)" - ver Figura 2.1. Deve-se ressaltar que a causa comum não é a falha de algum outro componente do mesmo sistema, uma vez que tais situações correspondem a um evento de falha única.

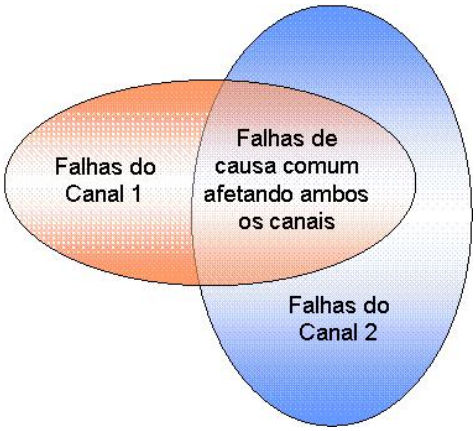


FIGURA 2.1: Relação entre FCC e as falhas individuais de cada canal

Conforme SANT´ANA (2006): "Uma FCC é o resultado de um evento, ocorrido em um tempo aleatório, o qual, em função das dependências, causa uma coincidência de estados de falha de componentes em dois ou mais canais separados de um sistema redundante, podendo levar à falha do sistema em realizar sua função pretendida".

Há muitas razões para a ocorrência de FCC. Citam-se, por exemplo:

- Erros de manutenção;
- Ambiente desfavorável (poeira, umidade, vibração, temperatura, etc.);
- Deficiência de projeto;
- Erro de operador;
- Eventos externos (incêndio, enchentes, terremotos, tornados, etc.).

Diversos modelos paramétricos têm sido propostos na literatura para a modelagem de falhas de causa comum, como por exemplo o modelo de Múltiplas Letras Gregas, modelo do Fator Alfa, e o modelo do Fator Beta. MOSLEH (1998) apresentam uma discussão mais detalhada sobre esses modelos. O modelo do Fator Beta tem sido bastante utilizado para falhas de causa comum. Possuindo apenas um parâmetro, é um modelo de fácil aplicação e com exigências bem mais brandas em termos de dados disponíveis do que outras opções, como o modelo de Múltiplas Letras Gregas.

A Norma IEC 61508 utiliza o Modelo do Fator Beta e apresenta as seguintes definições: o fator $\beta$ representa o percentual da taxa de falha total não detectada do componente considerada como falha de modo comum não detectada e o fator $\beta_D$ representa o percentual da taxa de falha total detectada do componente considerada como falha de modo comum detectada.

#### 2.3.2.3 Falha de Causa Comum - O Modelo do Fator Beta ($\beta$)

O modelo do fator $\beta$ para tratamento de falhas de causa comum foi introduzido por K. FLEMING (FLEMING 1975). Neste modelo, o fator $\beta$ consiste de um parâmetro em adição à probabilidade de taxa de falha comum. Isto quer dizer que, uma fração da taxa de falha do componente está associada com os eventos de causa comum que incidem sobre todos os componentes. Outra hipótese assumida é que sempre quando um evento de causa comum ocorre, todos os componentes dentro do mesmo grupo falham. Assim, para o grupo de componentes somente existem os eventos de falhas independentes de cada componente ou o evento de falha simultânea de todos os componentes.

O modelo do fator beta assume que os efeitos de causa comum podem ser representados no modelo de confiabilidade do sistema como uma proporção da probabilidade de falha de qualquer canal único de componentes múltiplos de sistemas redundantes. Onde os canais têm diferentes níveis de complexidade, o fator beta é aplicado à taxa de falha estimada ou à probabilidade do canal de maior confiabilidade (ANDREWS & MOSS 2002).

Considere-se um sistema composto de $n$ componentes idênticos, cada um com taxa de falha constante $\lambda$. A falha de um determinado componente pode ocorrer somente devido a uma dentre duas maneiras possíveis:

- Fatores relacionados somente ao componente em questão e, portanto, independentes da condição dos outros componentes do sistema; ou

- Fatores capazes de acarretar a falha simultânea de todos os componentes do sistema.

Seja $\lambda_i$ a taxa de falha devido à primeira causa (independente) e seja $\lambda_c$ a taxa de falha devido ao segundo tipo de causa (dependente - causa comum). Portanto, independência entre os dois tipos de causas de falha, a taxa de falha total $\lambda$ de cada componente é simplesmente a soma das taxas de falha dos dois tipos de causas:

$$\lambda = \lambda_i + \lambda_c \tag{2.1}$$

O fator $\beta$ é definido como a relação entre a taxa de falha comum e a taxa de falha total, ou seja, representa a proporção relativa de falhas de causa comum dentre todas as falhas de um componente (ver equação 5.69):

$$\beta = \frac{\lambda_c}{\lambda} \qquad \text{ou} \qquad \lambda cc = \beta \cdot \lambda \tag{2.2}$$

e

$$\lambda_i = \lambda - \lambda_c = (1 - \beta) \cdot \lambda \tag{2.3}$$

Cabe destacar que neste modelo, a probabilidade de ocorrerem falhas simultâneas de um número parcial de componentes é nula.

O Anexo D da Parte 6 da Norma IEC 61508 (IEC-61508-6 2000) apresenta uma metodologia para o cálculo de $\beta$ e $\beta_D$, sendo que esta metodologia é limitada a falhas de causa comum de *hardware* e baseada em julgamentos de engenharia e não abrange as falhas de causa comum causadas por *software* ou pela complexidade do processo.

### 2.3.3 Função Densidade de Probabilidade

A função densidade de probabilidade relaciona o valor de uma variável aleatória com a probabilidade dela assumir este determinado valor, ou faixa de valores no entorno do valor considerado. Para variáveis aleatórias discretas, a probabilidade de assumir

cada resultado é fornecido em uma função densidade de probabilidade. Para variáveis aleatórias contínuas, a função densidade de probabilidade fornece a probabilidade da variável assumir um valor aleatório no entorno do valor considerado (GOBLE 1998).

Para variáveis aleatórias discretas, a função densidade de probabilidade apresenta as seguintes propriedades:

$$P(x) \geq 0 \quad \text{para todo} \quad x$$

e

$$\sum_{i=1}^{n} P(x_i) = 1$$

e para variáveis aleatórias contínuas:

$$f(x) \geq 0 \quad \text{para todo} \quad x$$

e

$$\int_{-\infty}^{+\infty} f(x)dx = 1$$

E ainda, para uma contínua função densidade de probabilidade, a probabilidade de assumir um valor no intervalo $a$ e $b$ é igual a:

$$P(a \leq x \leq b) = \int_{a}^{b} f(x)dx$$

A probabilidade de falha durante qualquer intervalo do tempo de operação é dado pela função densidade de probabilidade, ou em outras palavras, esta função representa a variação da probabilidade de falha por intervalo de tempo. Esta função densidade de probabilidade (fdp) é definida como (GOBLE 1998):

$$f(t) = \frac{dF(t)}{dt} \tag{2.4}$$

e pode ser matematicamente descrita em termos da variável aleatória $T$:

$$f(t) = \lim_{\Delta t \to 0} P(t < T \leq t + \Delta t) \tag{2.5}$$

A expressão 2.5 pode ser interpretada como a probabilidade que o tempo de falha, $T$, irá ocorrer entre o tempo operacional, $t$, e o próximo intervalo da operação, $t + \Delta t$.

Na equação 2.4, $F(t)$ é a função acumulada de falhas e representa a probabilidade da falha ocorrer entre $t_1$ e $t_2$. Pode ser matematicamente expressa pela expressão:

$$F(t_2) - F(t_1) = \int_{t_1}^{t_2} f(t)dt \tag{2.6}$$

### 2.3.4 Função de Confiabilidade

Em confiabilidade, estamos preocupados com a probabilidade de que um item sobreviva a um dado intervalo estabelecido (de tempo, ciclos, distância). Isto é, não haverá falhas no intervalo de 0 a $t$. A confiabilidade é dada pela função de confiabilidade $R(t)$ e pode ser expressa conforme apresentado na equação 2.7:

$$R(t) = \int_{t}^{\infty} f(t)dt = 1 - \int_{-\infty}^{t} f(t)dt = 1 - F(t) \tag{2.7}$$

Logo, $F(t)$ é a probabilidade de falha do sistema, ou seja:

$$F(t) = 1 - R(t) \tag{2.8}$$

Conforme OLIVEIRA (2006), a probabilidade de um componente que funcione em $t = 0$ falhar até o instante $t + dt$ pode ser escrita como a soma das probabilidades de dois eventos disjuntos: (1) o componente falha até o instante $t$ e (2) o componente funciona até o instante $t$ e falha no intervalo $dt$ seguinte. Usando as definições de confiabilidade, $R(t)$ e da não-confiabilidade, F(t), pode-se escrever:

$$F(t + dt) = F(t) + [1 - F(t)]\lambda(t)dt \tag{2.9}$$

e rearranjando a equação 2.10, e fazendo $\Delta t = 0$:

$$F(t + dt) = F(t) + [1 - F(t)]\lambda(t)dt \tag{2.10}$$

$$\frac{dF(t)}{dt} = [1 - F(t)]\lambda(t) \tag{2.11}$$

A resolução da equação diferencial apresentada na equação 2.11 fornece a expressão da não-confiabilidade em função do tempo e da taxa de falha $\lambda$ do componente. Para

aplicarmos a integral, necessitamos de uma condição inicial, que é dada pela condição do componente no instante $t = 0$. Pela própria definição de $F(t)$ vemos que o componente está funcionando em $t = 0$. Portanto, podemos dizer que $P(t = 0) = 0$, daí:

$$\frac{dF(t)}{1 - F(t)} = \lambda(t)dt \tag{2.12}$$

integrando a equação 2.12, desde t = 0 até t, temos:

$$\int_0^t \frac{dF(t')}{1 - F(t')} = \int_0^t \lambda(t')dt' \tag{2.13}$$

e resolvendo a equação 2.13:

$$-ln[1 - F(t)] + ln[1 - F(0)] = \int_0^t \lambda(t)dt \tag{2.14}$$

como $P(0) = 0$ e $ln(1 - 0) = 0$, temos:

$$-ln[1 - F(t)] = \int_0^t \lambda(t)dt \tag{2.15}$$

que pode ser reescrita da seguinte maneira:

$$1 - F(t) = exp[-\int_0^t \lambda(t)dt] \tag{2.16}$$

ou seja:

$$F(t) = 1 - exp[-\int_0^t \lambda(t)dt] \tag{2.17}$$

e conforme apresentado na equação 2.8, é possível escrever a equação da confiabilidade como:

$$R(t) = exp[-\int_0^t \lambda(t)dt] \tag{2.18}$$

Conforme citado, a taxa de falha pode ser descrita como uma função tal que $\lambda(t)dt$ fornece a probabilidade de que um item (componente) que não falhou entre 0 e $t$, sofra uma falha entre $t$ e $t + dt$, ou ainda, conforme OLIVEIRA (2006), $\lambda(t)dt$ é a

probabilidade de que um componente que funcione em $t$ falhe entre $t + dt$ e a taxa de falha em $t$, $\lambda(t)$, é o limite desta probabilidade dividida por $dt$, quando $dt$ tende a zero. Esta função pode ser matematicamente descrita conforme a equação 2.19 a seguir:

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{f(t)}{1 - F(t)} \tag{2.19}$$

Considerando que o tempo de operação do componente seja curto comparado com seu tempo de vida útil, pode ser assumido um valor constante para a taxa de falha (OLIVEIRA, MELO, FLEMING & LIMA 1985). A confiabilidade passa a obedecer, então, a uma lei exponencial de falhas dada por:

$$R(t) = e^{-\lambda t} \tag{2.20}$$

Em um componente que segue a distribuição exponencial, a probabilidade dele falhar durante um intervalo de tempo fixado independe de quanto tempo o componente já tenha funcionado até o início do intervalo considerado. Esta é uma característica exclusiva da distribuição exponencial, e, por isso, diz-se que todo componente que segue a distribuição exponencial não envelhece, ou ainda, que esta distribuição não tem memória (OLIVEIRA et al. 1985).

# Capítulo 3

# Sistemas Instrumentados de Segurança - SIS

## 3.1 Introdução

Sistemas Instrumentados de Segurança (SIS) ou Sistemas de Intertravamento de Segurança ou Sistemas de Desligamento de Emergência (ESD), entre tantos outros nomes dados a eles, são uma classe de sistemas responsáveis pela segurança operacional de unidades e equipamentos industriais (BEGA et al. 2003). Eles causam a parada de emergência ou impedem uma operação insegura sempre que as condições de processo ultrapassam os limites pré-estabelecidos como seguros, ou que se estabeleçam condições operacionais perigosas.

Atualmente, em função do grande avanço da eletrônica digital da última década, os modernos sistemas de proteção usados na indústria utilizam unidades digitais para realização das suas lógicas de atuação, podendo combinar os sinais dos sensores de várias maneiras e executar acionamentos dos mais diversos tipos de acionadores redundantes, podendo assim, realizar complexas tarefas de intertravamento de segurança em equipamentos ou instalações que lidam com produtos ou processos perigosos. Portanto, SIS é uma designação genérica que engloba todos os sistemas de segurança que utilizam uma combinação qualquer de sensores (indicadores), unidade lógica e elementos finais (atuadores) para a realização de uma ou mais funções de segurança (CHAME, OLIVEIRA & DINIZ 2007).

Um SIS pode ter diferentes níveis de redundância em qualquer um dos seus três componentes básicos, possibilitando assim um grande número de configurações alternativas. Assim, qualquer dos três componentes básicos pode ser configurado com uma lógica do tipo *koon*, ou seja, a ação é executada quando pelo menos k dos n componentes existentes comandarem a execução da ação. As configurações mais encontradas em aplicações práticas na indústria são as do tipo 1oo1 (lê-se 1-de-1), 1oo2 e 2oo3, entretanto, outros tipos como 2oo2 e 1oo3 são também utilizadas em aplicações especiais. Recentemente, um novo CLP foi lançado no mercado com uma configuração do tipo 2oo4, o qual, segundo seu fabricante apresenta alto nível de confiabilidade tanto para falhas críticas como para falhas espúrias.

As Normas relacionadas, ANSI/ISA S84, IEC 61508 e IEC 61511, colocam requisitos claros quanto aos chamados níveis de integridade de segurança, mais conhecidos pela sigla SIL, do inglês, *Safety Integrity Level*. Os valores de SIL refletem os níveis de confiabilidade que devem ser fornecidos pelos SISs, no que se refere à sua função principal, que é a de cumprir uma dada função de segurança quando da ocorrência de um determinado evento perigoso. A ocorrência do evento perigoso é chamada de uma "demanda" do sistema de proteção. A resposta correta do SIS a uma demanda leva a instalação ao seu estado seguro, impedindo, assim, a ocorrência de um acidente. Por sua vez, a falha do SIS na demanda leva à ocorrência de um acidente, caso o SIS seja a única camada de proteção da instalação para a demanda do evento perigoso em questão.

O início do projeto de um SIS passa pela definição do SIL de cada malha de segurança. A definição do SIL pode ser feita através de várias técnicas quantitativas e qualitativas, e começa por uma análise de riscos do processo, onde se identificam os riscos envolvidos (BEGA et al. 2003). O conceito de SIL será discutido, na seção 3.4.

Este capítulo tem como intuito apresentar e discutir os conceitos relacionados aos Sistemas Instrumentados de Segurança (SIS), em particular o de Funções Instrumentadas de Segurança (FIS), Nível de Integridade de Segurança (SIL) e o enfoque do ciclo de vida da segurança, adotado pelas normas do IEC (IEC-61508 1998) e (IEC-61511 2003). Apresenta ainda uma breve descrição destas e de outras normas relacionadas ao assunto, bem como de outras referências metodológicas. É também dado destaque especial ao conceito de Probabilidade de Falha na Demanda (PFD), sendo de

fundamental importância a avaliação dos efeitos sobre o seu valor numérico em função da adoção de diferentes políticas de testes e dos diferentes níveis de redundância das configurações lógicas das várias partes de um SIS. Esta avaliação consiste em um dos principais objetivos deste trabalho, tendo em vista o impacto que exerce sobre os resultados das análises custo-benefício e, conseqüentemente, sobre a estratégia adotada para o atendimento a um determinado nível de SIL Requerido.

## 3.2 Função Instrumentada de Segurança - FIS

Uma definição típica de FIS utilizada na norma do IEC 61511 é "qualquer função implementada através de um SIS com o objetivo de prevenir ou mitigar determinado evento perigoso" (IEC-61511 2003). Alguns exemplos de FIS freqüentemente encontrados na indústria são: 1) atuação de bloqueio de fluxo de água quente para proteger contra alta temperatura ou alta pressão, 2) desligamento de uma bomba para impedir transbordamento de um tanque, 3) bloqueio de linha de gás em caso de detecção de gás na área, e 4) abertura de válvula de purga para flare em caso de fogo detectado na área.

Uma FIS pode também ser definida como um conjunto único de ações específicas e o correspondente equipamento necessário para identificar um perigo específico e atuar de forma a trazer o sistema para um estado seguro.

As FIS não devem ser vistas como a instrumentação que impede a planta de funcionar, e sim como a instrumentação que mantém a planta segura. Para levar este conceito para a planta, procedimentos de operação devem ser encarados como mais um modo de conseguir um produto de qualidade ou uma alta taxa de produção. As normas de SIS requerem que procedimentos de operação informem ao operador dos riscos específicos do processo e do potencial das conseqüências se os desvios de processo não são controlados.

## 3.3 Probabilidade de Falha na Demanda - PFD

Disponibilidade é um atributo de confiabilidade que, para sistemas reparáveis, pode ser definido como a probabilidade do sistema funcionar num determinado instante $t$, ou

ainda, a probabilidade do sistema estar apto a operar em um dado instante de tempo, nestes casos denominada disponibilidade instantânea. Por exemplo, se um equipamento qualquer pode operar por 98% do tempo disponível durante a sua vida útil, significa que o mesmo estará inoperante durante os 2% restantes.

Observe-se que para equipamentos de produção, este conceito já apresenta uma idéia quantitativa do que esperar do equipamento. Para sistemas de segurança, um conceito mais adequado é o de probabilidade de falha na demanda, porque muitas falhas não são detectadas imediatamente logo que ocorrem, podendo permanecer ocultas por longos períodos, até que se realize um teste que permita descobrí-las e, aí então, proceder ao seu reparo (BEGA et al. 2003). Se não for testado, a probabilidade de falha tende a 1.0 com o tempo (ver Figura 3.1). Testes periódicos mantêm a probabilidade de falha dentro do limite desejável (ver Figura 3.1, onde $\theta$ é o intervalo de teste).

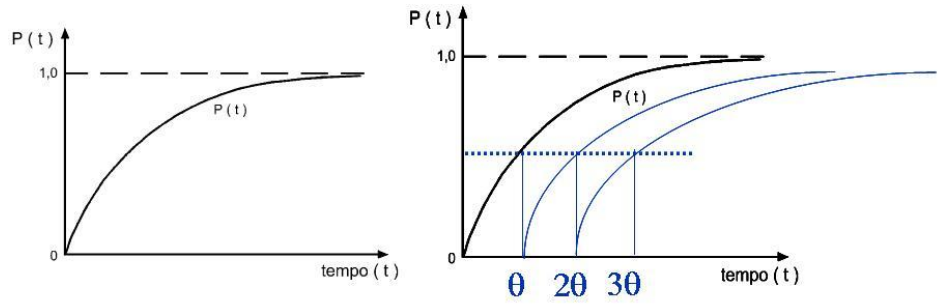


FIGURA 3.1: Testes Periódicos em Sistemas de Segurança

Desta forma, fica claro definir a Probabilidade de Falha na Demanda, ou PFD, como um atributo de confiabilidade que indica qual a probabilidade de um componente falhar em cumprir uma ação previamente especificada no momento em que ela for demandada. Conforme cita Finkel (BEGA et al. 2003), é possível dizer que especifica-se um Sistema Instrumentado de Segurança para se obter uma "performance estatística esperada", ou seja, para reduzir a possibilidade de acidentes a uma taxa considerada como aceitável e a PFD é o atributo que especifica este valor.

A PFD não depende da demanda em si, informando apenas qual a probabilidade do equipamento não funcionar adequadamente quando uma demanda ocorrer. Partindo do princípio de que poderá ocorrer um acidente sempre que houver uma demanda do SIS e ele estiver indisponível, o risco de acontecer um acidente fica então dependente da PFD e da freqüência da demanda.

A qualidade de um equipamento depende dele intrinsecamente, e não da demanda real de seu funcionamento, e, assim, a PFD permite que se compare o desempenho relativo de diferentes equipamentos ou configurações de equipamentos, independendo da aplicação desejada. É a aplicação, ou melhor, seus riscos, que definem qual a PFD aceitável para o equipamento a ser especificado ou escolhido para aquela aplicação específica.

De forma resumida então, é possível dizer que a efetividade de um SIS é medida através da sua "Probabilidade de Falha na Demanda" ou "Fator de Redução de Risco", e é classificada através de um índice chamado "Nível de Integridade de Segurança" (ou do inglês, *Safety Integrity Level* - SIL), definido pela IEC-61508, e descrito na seção 3.4. Em relação à disponibilidade, definida anteriormente nesta seção, é possível dizer que: $PFD = 1 - D$, onde D é a disponibilidade. O Fator de Redução de Risco, ou FRR, expressa a magnitude de redução de risco conseguida com a implementação de uma medida de redução de risco e pode ser definido como o inverso da PFD, ou seja, $FRR = 1/PFD$ (ver Tabela 3.2).

## 3.4 Nível de Integridade de Segurança - SIL

O SIL é definido como uma faixa de probabilidade de falha na demanda e representa uma magnitude da redução de risco que um sistema instrumentado de segurança (SIS) deve ser capaz de fornecer.

O SIL é o parâmetro-chave de projeto para a especificação do Fator de Redução de Risco (FRR) que um equipamento de segurança deve fornecer a uma função em particular. Se porventura, o SIL não for especificado, o equipamento em questão não poderá ser projetado adequadamente, tendo em vista que somente a sua ação será especificada. Para se projetar adequadamente uma FIS, dois tipos de especificações são requeridas: a especificação da função do equipamento e o seu nível de confiabilidade (PFD). O SIL é endereçado à segunda especificação, indicando a probabilidade mínima de funcionamento adequado do equipamento, ou seja, se o mesmo executará de forma correta a função para a qual foi projetado quando for solicitado (MARSZAL & SCHARPF 2002). Este SIL é também chamado de "SIL Requerido".

Os valores de SIL, ou Nível de Integridade de Segurança, variam de 1 a 4 nas Normas

do IEC ((IEC-61508 1998) e (IEC-61511 2003)) e de 1 a 3 na Norma da ISA (ANSI/ISA-84.00.01 2004) e refletem os níveis de confiabilidade que devem ser fornecidos pelos SISs, no que se refere à sua função principal, que é a de cumprir uma dada função de segurança quando da ocorrência de um determinado evento perigoso. A ocorrência do evento perigoso é chamada de uma "demanda" do sistema de proteção. A resposta correta do SIS a uma demanda leva a instalação para o seu estado seguro, impedindo assim, a ocorrência de um acidente. Por sua vez, a falha do SIS na demanda leva à ocorrência de um acidente, caso o SIS seja a única camada de proteção da instalação para a demanda do evento perigoso em questão.

Conforme será discutido mais adiante, as Normas do IEC ((IEC-61508 1998) e (IEC-61511 2003)) classificam os SISs de acordo com o regime de demandas a que estão submetidos: baixa freqüência de demandas e alta freqüência de demandas. Neste trabalho, apenas o regime de baixa demanda é considerado, dado ser este o mais importante para a indústria de processos.

Desta forma, o indicador de confiabilidade que é correlacionado aos níveis de SIL na Norma IEC 61508 (IEC-61508 1998) para regimes de baixa demanda, é a PFD. A relação entre os valores de SIL e da correspondente faixa de valores de PFD está indicada na Tabela 3.1.

TABELA 3.1: Relação entre o valor do SIL e a PFD considerando regime de baixa demanda

| SIL | PFD - Probabilidade de Falha na Demanda |
|---|---|
| 1 | $\geq 10^{-2}$ $a$ $< 10^{-1}$ |
| 2 | $\geq 10^{-3}$ $a$ $< 10^{-2}$ |
| 3 | $\geq 10^{-4}$ $a$ $< 10^{-3}$ |
| 4 | $\geq 10^{-5}$ $a$ $< 10^{-4}$ |

Conforme indicado anteriormente, os valores do SIL são fixados em função do nível de risco imposto pelo evento perigoso que gera a demanda pela atuação do SIS, variando de SIL 1 a SIL 4 em função da Probabilidade de Falha na Demanda (PFD) do SIS, conforme indicado na Tabela 3.1 extraída da Norma IEC 61508. Para se chegar ao SIL Requerido é necessário conduzir uma análise de risco específica para a sua função de segurança. A Norma apresenta vários métodos de análise de risco que podem ser usados para a determinação do SIL Requerido, abrangendo desde métodos puramente

qualitativos até análises quantitativas de risco. Um dos métodos mais utilizados é o do Gráfico de Risco, que será discutido posteriormente no Capítulo 4 deste trabalho.

O que afeta o SIL de uma FIS? O nível de integridade de segurança é afetado pelos seguintes parâmetros (SUMMERS 2002):

- Integridade do Componente (por exemplo, taxa de falhas e modos de falha);
- Redundância e votação;
- Intervalo funcional de teste;
- Cobertura de Diagnóstico - DC;
- Outras causas comuns (incluindo aquelas relacionadas ao componente/ dispositivo, projeto, fatores sistemáticos e erros humanos).

Os parâmetros integridade do componente/dispositivo, cobertura de diagnóstico e causa comum, são tipicamente limitados pelo dispositivo da Função Instrumentada de Segurança (FIS) e práticas de instalação. As exigências de redundância e intervalos funcionais de testes têm o maior impacto no projeto e nas práticas de operação/manutenção nas unidades de processo existentes (SUMMERS 2002).

Conforme já destacado, o SIL adequado para o SIS é o que faz com que o risco inerente ao processo seja igual ou menor que o nível de risco aceitável, proporcionando assim a segurança necessária para a operação da planta, sem esquecer que um bom projeto deve considerar também a disponibilidade operacional, não causando o desligamento da planta mais vezes do que o necessário. A Tabela 3.2 apresenta os valores de SIL em função da PFD, bem como em termos da disponibilidade (equivalente a $1 - PFD(\%)$), da PFD (em termos percentuais) e do fator de redução de risco.

TABELA 3.2: SIL em Função da Disponibilidade, da PFD e do FRR

| SIL | Disponibilidade desejada | PFD | FRR |
|---|---|---|---|
| 1 | $90,00 \quad a \quad 99,00\%$ | $1 \quad a \quad 10\%$ | 10 a 100 |
| 2 | $99,00 \quad a \quad 99,90\%$ | $0,1 \quad a \quad 1\%$ | 100 a 1000 |
| 3 | $99,90 \quad a \quad 99,99\%$ | $0,01 \quad a \quad 0,1\%$ | 1000 a 10.000 |
| 4 | $> 99,99\%$ | $> 0,01\%$ | $> 10.000$ |

Após o processo de definição do SIL Requerido, o enquadramento neste nível de integridade de segurança depende de vários fatores. Estes fatores estão relacionados com a qualidade dos instrumentos, o nível de diagnóstico de falha disponível para os componentes do SIS, o período entre testes, a qualidade destes testes, o nível de redundância e o arranjo (arquitetura) entre os instrumentos, etc.

## 3.5 Normas Relacionadas e Outras Referências Metodológicas

Uma norma técnica é um documento estabelecido por consenso e aprovado por um organismo reconhecido, que fornece para uso comum e repetitivo, regras, diretrizes ou características para atividades ou para seus resultados, visando à obtenção de um grau ótimo de ordenação em um dado contexto. Elas podem estabelecer requisitos de qualidade, de desempenho, de segurança (seja no fornecimento de algo, no seu uso ou mesmo na sua destinação final), mas também podem estabelecer procedimentos, padronizar formas, dimensões, tipos, usos, fixar classificações ou terminologias e glossários, definir a maneira de medir ou determinar as características, como os métodos de ensaio.

As normas internacionais são normas técnicas estabelecidas por um organismo internacional de normalização para aplicação em âmbito mundial. Existem diversos organismos internacionais de normalização, em campos específicos, como a ISO (a maioria dos setores), a IEC (área elétrica e eletrônica) e a ITU (telecomunicações).

Conforme já discutido, com o grande avanço da automação industrial na última década, os chamados Sistemas Instrumentados de Segurança passaram a representar um dos principais pilares da segurança de processo nas indústrias química, petroquímica e de óleo/gás. Por se tratarem de aplicações novas, para as quais não se dispunha de experiência prática significativa e pelo grande aumento da complexidade desse tipo de sistema de proteção, surgiram alguns questionamentos quanto ao nível efetivo de proteção proporcionado pelos SISs. Dado este cenário, várias normas sobre o desenvolvimento, projeto e manutenção dos SIS foram editadas. Entre estas estão as do IEC, como a IEC-61508 (voltadas para indústrias em geral) e a IEC 61511 (para indústrias de processamento contínuo, líquidos e gases) e a da ISA, a ANSI/ISA-S.84.01, semelhante

à do IEC 61511, porém, mais voltada para o SIS propriamente dito, enquanto a IEC 61511 dá ênfase a análise de risco e às outras camadas de proteção (mais abrangente).

No Brasil, ainda em função deste avanço da automação industrial, em 1997, a PETROBRAS elaborou a Norma PETROBRAS CONTEC N-2595 - Critérios de Projeto e Manutenção para Sistemas Instrumentados de Segurança em Unidades Industriais, para uso nas instalações da PETROBRAS.

A característica mais marcante destas normas é que são normas voltadas para a performance exigida do sistema, e não normas prescritivas. Isso quer dizer que desde que o usuário (ou projetista) atinja o nível de segurança desejado (SIL), qualquer tecnologia é aceitável, e o nível de redundância, bem como o intervalo de teste, ficam a critério de quem especifica o sistema, embora ambos estejam intimamente relacionados com o SIL pretendido. De acordo com Finkel (BEGA et al. 2003), se por um lado, esta característica aumenta a "durabilidade" da norma, fazendo com que ela não precise ser revisada cada vez que uma nova tecnologia comece a ser empregada, por outro lado, não tendo "receita de bolo" aumenta a responsabilidade de quem as usa. Exceção a este respeito é a Norma da Petrobras, N-2595, que é bastante prescritiva, mostrando uma grande preocupação em se classificar cada malha, e depois definindo qual tecnologia aplicar para cada classe de risco.

Esta seção tem o objetivo de abordar nas subseções subseqüentes, uma descrição mais detalhada de cada uma das principais normas e referências relacionadas ao tema deste trabalho.

### 3.5.1 Normas IEC

A IEC (*International Electrotechnical Commission*), é uma organização mundial, não-governamental, criada em 1906, para padronização. Seu objetivo é promover co-operação internacional em todas as questões que envolvem padronização no campo elétrico e eletrônico. Pode-se dizer que é o organismo internacional de normalização para a área elétrica, eletrônica e de tecnologia relacionada. Para este fim e em conjunto com outras atividades, a IEC publica normas internacionais.

As normas IEC são desenvolvidas nas suas comissões técnicas (IEC/TC), que são organizadas numa base temática com representantes dos seus membros. As repre-

sentações são nacionais. A aprovação das normas IEC é feita mediante votação entre os seus membros. A participação brasileira nos trabalhos de normalização da IEC é efetuada através da ABNT (Associação Brasileira de Normas Técnicas). As Normas IEC são voluntárias, cabendo aos seus membros decidirem se as adotam como normas nacionais ou não. A adoção de uma norma IEC como norma brasileira recebe a designação NBR IEC.

A seguir são detalhadas as duas principais normas do IEC relacionadas ao tema deste trabalho: IEC 61508 e a IEC 61511.

#### 3.5.1.1 IEC 61508

A norma internacional IEC 61508 foi criada com o objetivo de atender mundialmente às necessidades de segurança, frente a uma crescente demanda de produtividade e tecnologia por parte de diversos segmentos industriais. Embora a sua aplicação não seja obrigatória em muitos países, como é o caso do Brasil, de acordo com a IEC 61508-1: Cláusula 1.4 (ver (IEC-61508-1 1998)), a IEC 61508 é uma publicação básica de segurança que será utilizada pelos comitês técnicos na preparação de normas (ROQUE 2006).

Esta norma começou a ser desenvolvida em 1984, pelo Comitê Técnico 65 da IEC, quando o foco era uma norma para *softwares* seguros. Deste ponto em diante, outros pontos foram sendo levantados como: e a parte do *hardware*?, e as falhas sistemáticas? ciclo de vida de segurança? Em 1995, a norma foi dividida em 7 partes, normativas e informativas. Em 1998, as partes 1, 3, 4 e 5 foram aprovadas como Normas Internacionais e em 1999, as partes 2, 6 e 7 foram aprovadas. No total, foram quase 15 anos desde o início do seu desenvolvimento até a aprovação total da norma atualmente disponível.

A IEC 61508 é uma norma que pode ser aplicada diretamente a qualquer processo industrial que utilize produtos e sistemas de segurança E/E/PE (elétricos/eletrônicos e eletrônicos progamáveis), independente do tipo de aplicação a que se destine. Pode também ser descrita como uma norma genérica, dividida em 7 partes, descritas como normativas, o que significa que elas são o padrão propriamente dito e contém exigências que devem ser atendidas. Alguns dos anexos, entretanto, são descritos como informativos, sob a ótica de que os mesmos não são exigências, mas sim guias que podem ser

utilizados durante a implementação das partes normativas. Deve ficar claro, entretanto, que as a maioria das partes 5, 6 e 7 são anexos informativos. As partes 1-3 são as partes principais e as partes 4-7 provêm material suplementar. A seguir são listadas todas as 7 partes da norma:

- **Parte 1**: *General Requirements*
- **Parte 2**: *Requirements for Electrical/Electronic/Programmable Electronic Safety-Related Systems*
- **Parte 3**: *Software Requirements*
- **Parte 4**: *Definitions and Abbreviations*
- **Parte 5**: *Examples of Methods for the Determination of Safety Integrity Levels*
- **Parte 6**: *Guidelines on the Application of IEC 61508-2 and IEC 61508-3*
- **Parte 7**: *Overview of Techniques and Measures*

A Norma IEC 61508 traz embutida em si dois conceitos que são fundamentais para a sua aplicação: o primeiro é o próprio conceito de SIL e o segundo é o do "ciclo de vida da segurança" (*safety life cycle model*), com o objetivo de ilustrar que a integridade de um SIS não é limitada à integridade do projeto, mas também é função do projeto, da operação, dos testes e da manutenção.

Desta forma, é possível dizer que a IEC 61508 (IEC-61508 1998) se consolidou pela introdução dos conceitos de ciclo de vida de segurança, pelos critérios de performance SIL e pelas considerações sobre especificações de *hardware* (IEC-61508-2 2000) e *software* (IEC-61508-3 1998) dos sistemas relacionados à segurança. Conforme ROQUE (2006), estas últimas características juntamente com o seu caráter genérico de aplicação, a tornaram mais conhecida como uma norma para fabricante e fornecedores de sistemas relacionados à segurança.

O objetivo da IEC 61508 de ser uma norma de segurança internacional unificada, não foi alcançado neste setor, mas ela serviu de base para que a norma IEC 61511 (IEC-61511 2003) fosse elaborada e atingisse esta meta. A Figura 3.2 apresenta as principais normas do IEC que já foram aprovadas e que utilizaram a Norma IEC 61508 como base para o seu desenvolvimento.

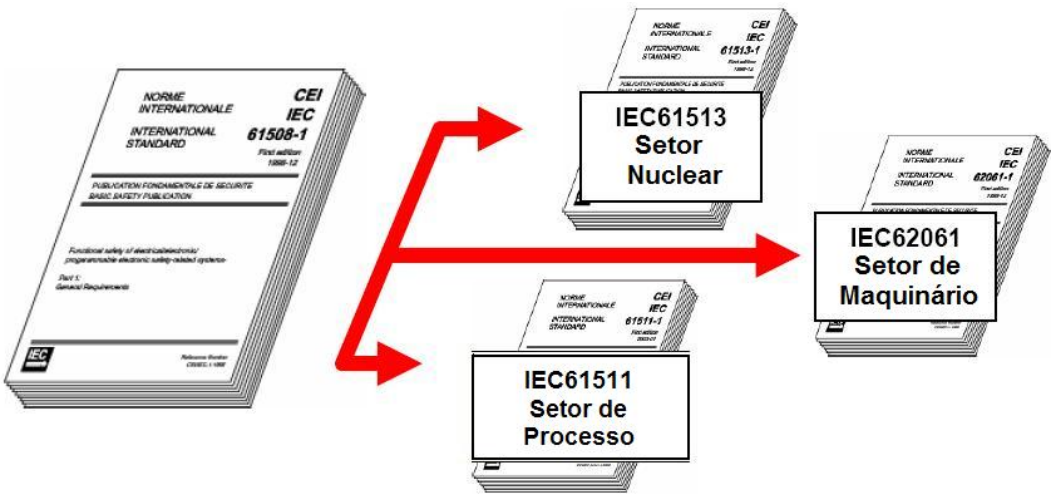


FIGURA 3.2: Normas IEC 61508 e 61511

#### 3.5.1.2 IEC 61511

Conforme citado anteriormente, a Norma IEC 61508 serviu de base para o desenvolvimento da Norma IEC 61511. Os membros participantes do desenvolvimento desta norma incorporaram as boas práticas de engenharia da IEC 61508, as suas próprias normas nacionais, referências e suas experiências no setor de processo (MAGGIOLI 1999).

A norma IEC 61511 é do tipo orientada à performance. Diferentemente das normas prescritivas, ela não está focada em especificar sistemas, parâmetros ou condições técnicas para determinadas aplicações. Norteia-se pelo princípio básico de que "quanto maior o nível de risco do processo, tanto melhor deverá ser a *performance* do sistema E/E/PE relacionado à segurança". Enquanto a IEC 61508 está dividida em 7 partes, a IEC 61511 tem apenas 3 partes, conforme listado abaixo:

- **Parte 1**: *General framework, definitions, bibliography, and system/software/ hardware requirements.*

- **Parte 2**: *Guidelines in the application of Part 1.*

- **Parte 3**: *Guidelines in the application of Hazard and Risk Analysis*

A IEC 61511 foi lançada no início de 2003 e em relação à sua divisão, é possível dizer que a parte 1 pode ser descrita como normativa, enquanto as partes 2 e 3, descritivas. A Parte 1 cobre o "ciclo de vida" incluindo: gerenciamento da função de segurança,

Análise de Riscos e Perigos, e as etapas desde o projeto até o descomissionamento do SIS. A Parte 2 apresenta orientações gerais para o uso da Parte 1, numa base "parágrafo por parágrafo"; enquanto a Parte 3, apresenta orientações mais detalhadas para o atendimento ao SIL e possui um certo número de anexos que cobrem metodologias qualitativas e quantitativas.

As mudanças principais na terminologia de uma norma para a outra podem ser vistas como uma tentativa de adaptar o texto para o setor de processo, por exemplo:

- IEC 61508 "E/E/PE safety function" para "safety instrumented function" (SIF);
- IEC 61508 "E/E/PE safety-related system" ou "PES" para "safety instrumented system" (SIS);
- IEC 61508 "equipment under control (EUC)" para "process";
- IEC 61508 "process control system" para "basic process control system (BPCS)".

### 3.5.2 Normas ISA

A ISA - *The Instrumentation, Systems, and Automation Society* é uma entidade mundial que estabelece normas, padrões e práticas indicadas para o setor de automação e controle. Atualmente estão em vigor, ou sendo atualizadas, cerca de 134 normas, que buscam a atividade de automação e controle segura, eficiente e rápida. As normas da ISA são, inclusive, incorporadas por outras entidades, que acabam aproveitando seu conteúdo para a elaboração de padrões específicos.

Por meio desta norma são padronizados os níveis de segurança para instalações industriais. O escopo do trabalho do comitê consiste em (PEREIRA & ALIPERTI 2006):

- Definir uma metodologia que seja peculiar aos sistemas eletrônicos programáveis de alta confiabilidade;
- Estabelecer critérios para e meios de avaliar a confiabilidade e disponibilidade em aplicações práticas;
- Prover diretrizes de especificação gerais que facilitem a compreensão;

- Prover diretrizes para aplicações de segurança que requerem alta confiabilidade;
- Desenvolver diretrizes para configurações de *hardware/software* específicas que podem ter níveis variados de confiabilidade e disponibilidade.

O propósito do trabalho consiste em escrever padrões para a utilização de Sistema Eletrônicos Programáveis (PES) em aplicações de segurança. É adotada a mesma terminologia E/E/PES no que tange aos sistemas instrumentados de segurança (SIS), nomeando os sensores, a lógica e os elementos finais de forma similar ao IEC 61511 (SMITH & SIMPSON 2004).

A situação atual é que o Comitê da ISA-SP84 publicou a ANSI/ISA-84.00.01-2004 Partes 1-3 (IEC 61511 Mod), Segurança Funcional: Sistemas Instrumentados de Segurança e o Setor da Indústria de Processo. Conforme PEREIRA & ALIPERTI (2006), esta série de 3 partes oferece exigências para a especificação, projeto, instalação, operação e manutenção de um sistema instrumentado de segurança, de forma que possa, de maneira confiável, se colocar ou manter um processo em situação segura. A ISA-SP84 está atualmente desenvolvendo vários relatórios técnicos para prover orientação na implementação e no uso da série de três partes da norma.

A primeira versão da norma é a ANSI/ISA-S84.01-1996, publicada em 1996 nos EUA e adotada por várias comunidades de segurança da indústria de processos e foi substituída pela ANSI/ISA-84.00.01-2004. Esta última versão é a mesma norma que a Norma IEC 61511 com uma cláusula denominada *"Grandfather Clause"*. Esta cláusula permite aos usuários manter o seu Sistema Instrumentado de Segurança (SIS), que foi projetado com as boas práticas de engenharia anteriores, sem ter necessidade de atualizar o SIS para a norma atual, ou seja, garante à empresa a possibilidade de manter seus antigos projetos de equipamentos com boas práticas de engenharia reconhecidas e aceitas, enquanto a companhia garantir que o SIS está projetado, mantido, inspecionado, testado e operado de maneira segura. A *Grandfather Clause* é somente uma frase; a premissa básica é que se deve ter um documento que garanta que o SIS foi avaliado e que determinou que o SIS garante que o processo irá operar de maneira segura (KLEIN 2005).

Esta norma considera apenas 3 níveis de SIL, equivalentes a SIL 1, 2 e 3 do padrão apresentado pelo IEC 61508 (ver Tabela 3.1), ou seja, valores de integridade maiores

que um valor de PFD de $10^{-4}$ não são consideradas.

### 3.5.3 PETROBRAS N-2595

Conforme citado, no Brasil, ainda em função deste avanço da automação industrial, em 1997, a PETROBRAS elaborou a Norma *PETROBRAS CONTEC N-2595*, para uso nas instalações da PETROBRAS. Esta norma já foi revisada duas vezes, sendo a primeira revisão datada de Julho de 2002 (Rev. A) e a segunda, datada de Outubro de 2002 (Rev. B).

Conforme cita Finkel (BEGA et al. 2003), um ponto de divergência entre a N-2595 e as outras normas é que quase todas as normas recomendam a total separação entre os sistemas de controle e os SIS, mas a N-2595 recomenda para os níveis de risco menores o uso do próprio SDCD (Sistema Digital de Controle Distribuído - elemento da área de automação industrial que tem como função primordial o controle de processos) para fazer um papel de SIS, reservando a equipamentos mais especializados e adequados às funções de segurança a proteção de malhas envolvendo riscos maiores. A natureza prescritiva da norma traz como vantagens uma certa forma de padronização entre sistemas projetados em unidades diferentes com pessoal de formação diferente, ou com vários níveis de entendimento de como projetar um SIS.

A N-2595 permite que o usuário abra exceções quanto à tecnologia escolhida para cada nível de risco, desde que justifique o porquê frente aos órgãos competentes da PETROBRAS, o que pode induzir o usuário a evitar os desvios das recomendações da norma.

A Norma N-2595 é apresentada em um volume único e em termos de metodologia é dividida em duas etapas, assim denominadas: classificação das malhas de segurança de acordo com a possibilidade de falhas na demanda e classificação das malhas de segurança de acordo com a possibilidade de falhas espúrias. Malha de Segurança é definida pela norma como "conjunto de um ou mais iniciadores, executor da lógica e um ou mais atuadores, com a função de prevenir determinado perigo".

A primeira etapa da metodologia proposta pela norma tem como objetivo principal determinar o SIL requerido para a malha de segurança, utilizando uma metodologia semi-qualitativa baseada em gráficos de risco que levam em consideração conseqüências

para a segurança pessoal, meio ambiente e perda de produção e equipamentos. A segunda parte objetiva verificar a necessidade de estabelecer tolerância das malhas de segurança a falhas espúrias, levando em consideração o retorno de 1 ano para a amortização dos investimentos, a perda de produção associada e as possíveis conseqüências relacionadas ao desarme do equipamento.

Cabe destacar que uma falha espúria podem ser definida como uma "falha cujo resultado implica na ação de pelo menos um atuador, sem que tenha ocorrido realmente um evento iniciador que o demandasse" e falha na demanda como uma "falha que se caracteriza pela não ação ou ação incorreta de pelo menos um atuador, quando da ocorrência de um evento iniciador que demande esta ação" (PETROBRAS 2002).

### 3.5.4 Normas DIN V

As Normas alemãs DIN V foram publicadas para sistemas de segurança e também foram usadas como uma das referências para as normas do IEC. Antes da publicação do IEC 61508, as normas alemãs DIN V 19250 e VDE 0801 eram usadas para a certificação de produtos. Cabe ressaltar que atualmente elas devem ser usadas em conjunto com a IEC 61508 (SMITH & SIMPSON 2004).

As normas alemãs DIN V 1950 e DIN V VDE 080 foram durante muito tempo adotadas como padrão por muitas comunidades de segurança (Europa, EUA, entre outros). Nesta época estas normas eram consideradas suficientemente completas para os projetistas e usuários de sistemas de segurança eletrônicos programáveis.

Na Alemanha, a metodologia de definição de riscos para indivíduos está estabelecida na DIN V 19250 (DIN-VDE-19250 1998). Esta norma estabelece o conceito de que sistemas de segurança devem ser projetados para encontrar determinadas classes, denominadas Classe 1 (AK1) até Classe 8 (AK8). A escolha da classe é dependente do nível de risco gerado pelo processo. A Norma DIN V 19250 força o usuário a considerar o perigo envolvido em seus processos e em determinar a integridade da segurança requerida do sistema.

A Norma VDE 0801 também é baseada em ciclo de vida e lida com métodos que objetivam evitar erros no desenvolvimento de ambos, *hardware* e *software*. Esta norma utiliza as categorias de risco da DIN V 1950 (Classes AK 1 a AK 8).

### 3.5.5 SINTEF

SINTEF é uma Fundação para Pesquisa Científica e Industrial do Instituto de Tecnologia Norueguês, localizado em Trondheim, Noruega. PDS, do norueguês "Palitelighet av Datamaskinbaserte Sikkerhetssystemer" significa "Confiabilidade e Disponibilidade de Sistemas de Segurança baseados em Sistemas Computadorizados".

O SINTEF desenvolveu um método de previsão de confiabilidade, apresentado no "PDS Method Handbook" (HAUGE, HOKSTAD, LANGSETH & OIEN 2006) e dados de confiabilidade, apresentados no "PDS Data Handbook" (HAUGE, LANGSETH & ONSHUS 2006), para a quantificação da indisponibilidade de segurança e perda de produção relacionadas a Sistemas Instrumentados de Segurança (SIS). Os dados de confiabilidade apresentados no "PDS Data Handbook" podem ser utilizados para o cálculo do SIL, de acordo com a Norma do IEC 61508. O método e os dados do PDS são amplamente utilizados na indústria *offshore*, mas são também aplicáveis para outro setores da indústria. Estas referências são constantemente atualizadas através do Fórum PDS.

O Fórum PDS foi iniciado em 1995 com o objetivo de atualizar os projetos de Pesquisa e Desenvolvimento do PDS. O principal objetivo é manter um fórum profissional para desenvolvimento de sistemas de segurança na indústria de petróleo e para a troca de experiência entre as companhias de óleo e gás, vendedores, empresas de engenharia, consultores, órgãos governamentais e organizações de pesquisa. As seguintes empresas são participantes do Fórum PDS:

- **Companhias de Óleo/Operadores**: A/S Norske Shell, BP Norge, Eni Norge, Norske Hydro ASA, PGS Production, ConocoPhillips Norge, Statoil ASA e TOTAL E&P Norge;

- **Vendedores/Fornecedores de Sistemas de Controle e Segurança**: ABB, FMC Kongsberg Subsea, Honeywell, Invensys Systems Norge, Kongsberg Maritime, Saas System, Siemens e Simrad Optronics;

- **Empresas de Engenharia e Consultores**: Aker Kvaener Engineering & Technology, Det Norske Veritas, Nemko, Safety Nordic e Scandpower Risk Management;

- **Órgãos Governamentais**: Petroleum Safety Authority Norway e Directorate for Civil Protection (observador) e Emergency Planning (observador).

## 3.6 Ciclo de Vida de Segurança

Uma definição de ciclo de vida de segurança, ou do inglês *Safety Lifecycle*, é que o mesmo é um processo de engenharia que utiliza etapas específicas para garantir que o sistema instrumentado de segurança (SIS) é efetivo na sua missão chave de redução de risco, bem como custo-eficiente em relação à vida do sistema (GOBLE & CHEDDIE 2005).

Conforme citado anteriormente, um dos principais conceitos que a Norma IEC 61508 (IEC-61508 1998) traz embutida em si e que é fundamental para a sua aplicação é o do "ciclo de vida da segurança".

O conceito do ciclo de vida da segurança forma o arcabouço central que aglutina a maioria dos conceitos da norma e que, sem dúvida, constitui-se em uma boa prática de engenharia para o tratamento de SISs. De uma forma simplificada, esse conceito engloba três fases distintas: análise, implementação e operação, ilustrados na Figura 3.3, extraída da norma.

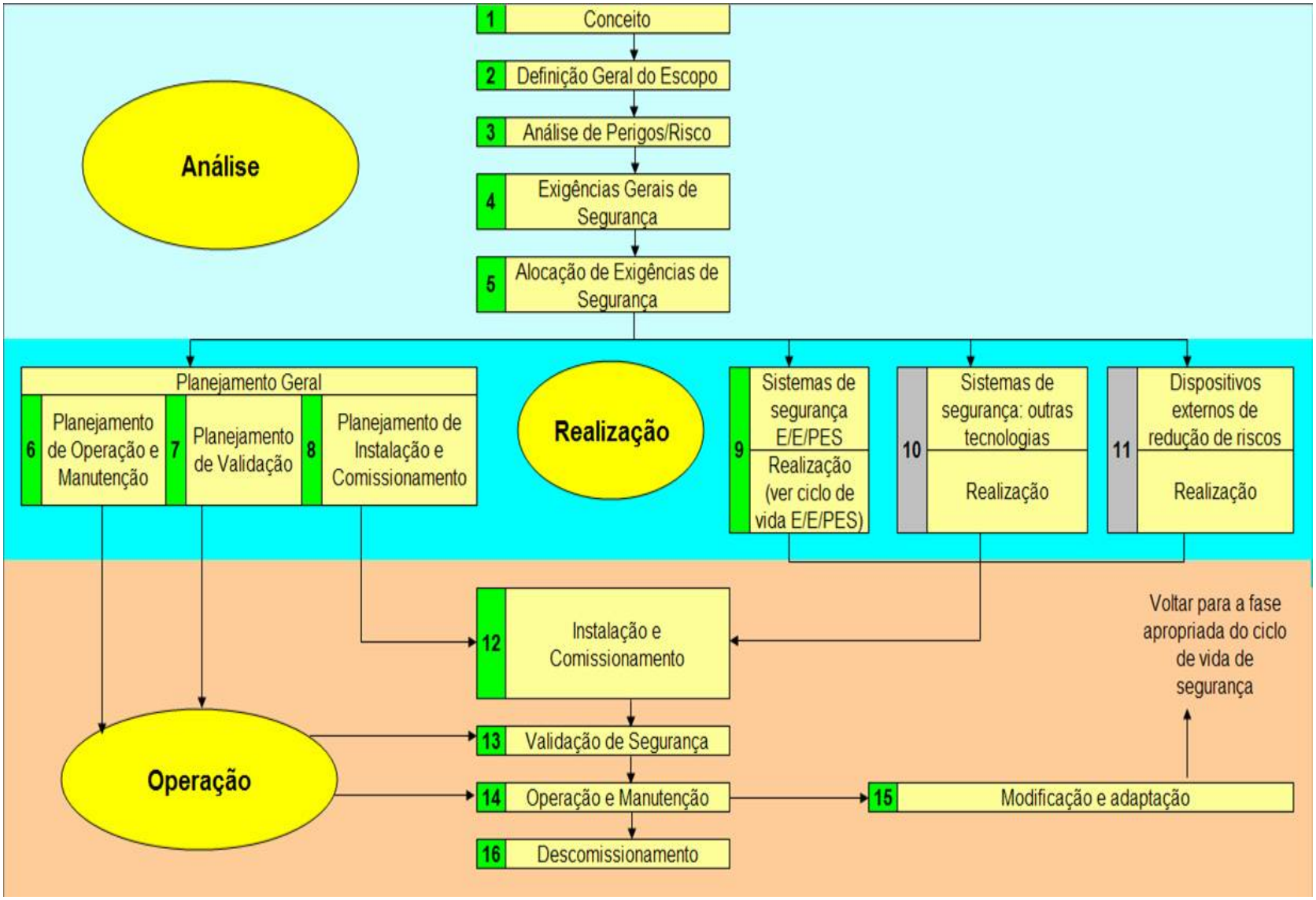


FIGURA 3.3: Ciclo de Vida de acordo com a IEC 61508

De uma forma simplificada, o conceito embutido no ciclo de vida da segurança pode ser representado pelos três passos ilustrados na Figura 3.4.


FIGURA 3.4: Fases do Ciclo de Vida - IEC 61508

- **Fase de Análise**: Analisar o Problema;
- **Fase de Implementação**: Projetar a Solução;
- **Fase de Operação**: Garantir a manutenção do nível de proteção do sistema durante toda a sua vida operacional.

Conforme citado anteriormente, é possível dizer que o início do projeto de um SIS passa pela definição do SIL de cada malha de segurança. A definição do SIL pode ser feita por várias técnicas quantitativas e qualitativas, e começa por uma análise de riscos do processo, onde se identificam os riscos envolvidos. A Fase de Análise consiste em se identificar e avaliar o risco, estimar a redução de risco necessária e determinar o SIL Requerido para cada FIS do SIS. Ou seja, por este conceito, inicialmente, os requisitos de desempenho do SIS são estabelecidos através do SIL requerido, através de uma análise de risco e de considerações sobre outras camadas de proteção existentes além daquela provida pelo SIS. Esta é a Fase de Análise indicada na Figura 3.4, ou seja, em outras palavras esta fase consiste em se identificar e avaliar o risco, estimar a redução de risco necessária e determinar o SIL Requerido para cada FIS do SIS.

Na Fase de Implementação (referida na Norma do IEC (IEC-61508 1998) como *Realization Phase*), de posse do SIL Requerido, faz-se o projeto do SIS e o planejamento para a Fase de Implementação. Para a execução do projeto, é necessário considerar

todas as alternativas de implementação que incluem, além da escolha do nível de redundância de cada parte do sistema, outras possibilidades, tais como, o estabelecimento dos intervalos entre testes do sistema, o fator de cobertura do diagnóstico, as defesas contra as falhas de causa comum e a possibilidade de uso de testes parciais (*partial stroke testing*). É nesta fase que os responsáveis pela implementação devem lançar mão das equações fornecidas no Volume 6 da Norma (IEC-61508 1998), para avaliar as PFDs das várias alternativas. Cabe ressaltar que estas equações estão deduzidas na seção 5.6.

As atividades previstas para a terceira fase, Fase de Operação, visam garantir que o nível de proteção fornecido pelo SIS seja mantido durante toda a vida do sistema, desde a sua instalação até o seu descomissionamento, passando pelas atividades de operação e manutenção do sistema. Nesta fase, devem também ser coletados dados de campo para se fazer uma validação geral das análises realizadas nas fases anteriores, ajustando-se as condições do sistema em função dos resultados dessa validação. Esta fase não é objeto do presente trabalho.

Como mostrado na Figura 3.4, em todas as fases do ciclo de vida de segurança, a Norma requer que todas as atividades sejam devidamente documentadas e que essa documentação seja mantida sob controle durante toda a vida operacional do sistema.

## 3.7 Restrições de Arquitetura dos Sistemas de Segurança de acordo com a Norma IEC 61508

Uma vez obtidos os resultados das PFDs de cada componente da malha de segurança, estes devem ser combinados de forma a verificar se o SIL da malha de segurança atende ao SIL requerido pela função de segurança. No entanto, para que esta verificação esteja de acordo com a Norma IEC 61508, devem-se também considerar as restrições impostas pela norma quanto ao máximo nível de integridade (SIL) atingível por uma malha de segurança em função das características dos seus componentes. Estas restrições impostas pela norma, são conhecidas como "Restrições de Arquitetura".

Além da exigência de um valor médio de PFD para um SIL, a Norma IEC 61508 traz este conceito de restrições de arquitetura. Este conceito adiciona exigências em

equipamentos que fazem parte da FIS. De acordo com (BEURDEN & BEURDEN-AMKREUTZ 2004), as restrições de arquitetura são expressas no nível requerido de Tolerância à Falha de *Hardware* (ou do inglês, *Hardware Fault Tolerance* - HFT). O nível requerido de Tolerância à Falha de *Hardware* é função da Fração de Falha Segura (ou do inglês, *Safe Failure Fraction* - SFF), do tipo do equipamento e do SIL desejado.

A seção denominada "Exigências para Integridade de Segurança de *Hardware*" da Parte 2 da Norma IEC 61508 (IEC-61508-2 2000) apresenta as restrições de arquitetura que devem ser levadas em consideração para a determinação do nível de integridade de segurança máximo que pode ser assumido por uma função de segurança. É possível verificar que o maior valor de SIL que pode ser assumido para uma função de segurança é limitado pela Tolerância à Falha de *Hardware* (HFT) e pela Fração de Falha Segura (SFF) dos subsistemas que desempenham aquela função de segurança.

Tolerância à Falha é definido como a capacidade de uma unidade funcional de continuar a desempenhar sua função de segurança requerida na presença de uma falha (LAYER 2004). Por exemplo, Tolerância à Falha de *Hardware* de $N$ significa que $N+1$ falhas podem causar a perda da função de segurança. Assim, o esquema de votação 1oo1 tem HFT igual a 0 (único canal), os esquemas 1oo2 e 2oo3 têm HFT igual a 1 (redundante), e o esquema 1oo3 tem HFT igual a 2 (dupla redundância).

A Fração de Falhas Seguras (SFF) de um subsistema é definida como uma fração de toda a falha de *hardware* de um componente que resulta ou em uma falha segura ou uma falha perigosa detectada, ou seja:

$$SFF = \frac{\lambda_{SD} + \lambda_{SU} + \lambda_{DD}}{\lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}} \tag{3.1}$$

e considerando que $\lambda$ corresponde à taxa de falha total do sistema, é possível destacar que: $\lambda = \lambda_{SD} + \lambda_{SU} + \lambda_{DD} + \lambda_{DU}$, ou seja, a taxa de falha total do sistema é igual ao somatório de falhas seguras detectadas, seguras não detectadas, perigosas detectadas e perigosas não detectadas.

Cabe ressaltar que o fator diagnóstico de cobertura (DC) do sistema é levado em consideração no cálculo da probabilidade de falha perigosa e na fração de falha segura (SFF), enquanto que a SFF é levada em consideração na determinação das restrições de arquitetura para a integridade de segurança do *hardware*.

Após a determinação da HFT e da SFF do sistema em análise, é necessário classificar cada componente da função de segurança quanto ao tipo de arquitetura: "Tipo A" ou "Tipo B". Um equipamento do Tipo A é definido como aquele que tem seus componentes com seus modos de falha bem definidos, e que o comportamento numa falha é completamente determinado, em que há dados suficientes para validar as taxas de falhas seguras e perigosas. Um equipamento Tipo B é definido como aquele que tem pelo menos um de seus componentes cujos modos de falha não estão bem definidos, ou que o comportamento numa falha não pode ser completamente determinado, ou que não há dados suficientes para validar as taxas de falhas seguras e perigosas. Normalmente válvulas, sensores e relés são do tipo A, enquanto transmissores e PLCs são do tipo B. Todos estes parâmetros são combinados e podem ser analisados nas tabelas 3.3 e 3.4 extraídas da Norma IEC 61508. Cabe ressaltar que "Não Permitido" na Tabela 3.4 significa que não é possível atribuir um SIL para um equipamento que apresente um valor de HFT de zero e um valor de SFF menor que 60%.

Tabela 3.3: Arquitetura Tipo A

| Fração de Falha Segura (SFF) | HFT | | |
|---|---|---|---|
| | 0 | 1 | 2 |
| $< 60$ | SIL 1 | SIL 2 | SIL 3 |
| $60\% - < 90\%$ | SIL 2 | SIL 3 | SIL 4 |
| $90\% - < 99\%$ | SIL 3 | SIL 4 | SIL 4 |
| $\geq 99$ | SIL 3 | SIL 4 | SIL 4 |

Tabela 3.4: Arquitetura Tipo B

| Fração de Falha Segura (SFF) | HFT | | |
|---|---|---|---|
| | 0 | 1 | 2 |
| $< 60$ | Não Permitido | SIL 1 | SIL 2 |
| $60\% - < 90\%$ | SIL 1 | SIL 2 | SIL 3 |
| $90\% - < 99\%$ | SIL 2 | SIL 3 | SIL 4 |
| $\geq 99$ | SIL 3 | SIL 4 | SIL 4 |

Assim, conforme apresentado, a determinação do SIL de uma FIS não depende somente da PFD calculada, mas também das restrições da norma apresentadas nas tabelas 3.3 e 3.4, ou seja, para atendimento à Norma do IEC 61508, o SIL atingido de uma função instrumentada de segurança é determinado pelo menor dos dois SILs

calculados: SIL baseado no cálculo da probabilidade de falha na demanda e o SIL baseado nas restrições de arquitetura. A Figura 3.5 (BEURDEN & BEURDEN-AMKREUTZ 2004), representa esta avaliação.

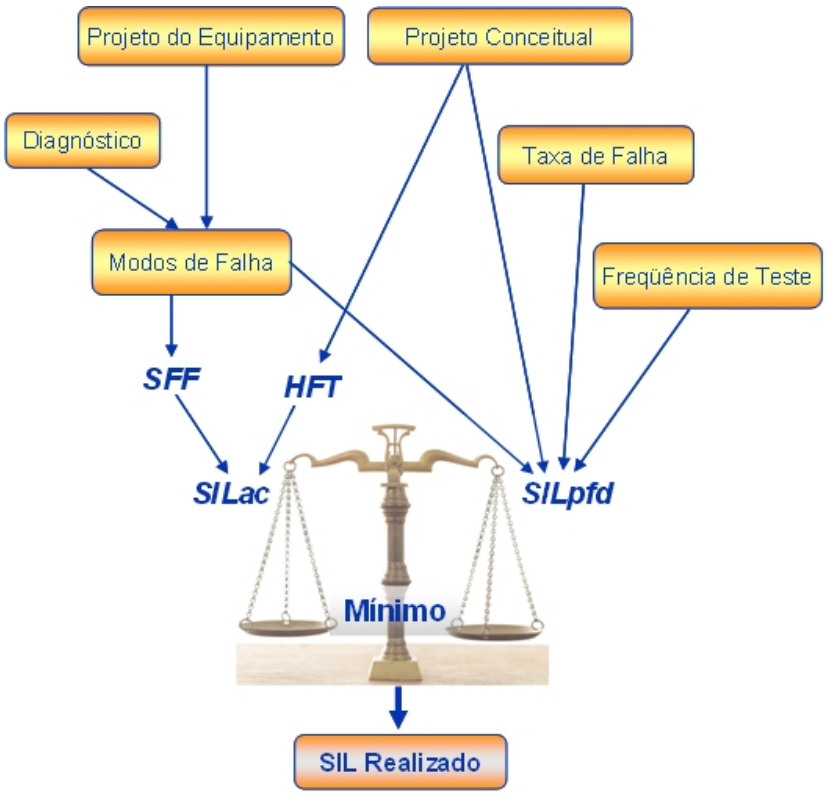


FIGURA 3.5: Mínimo SIL

# Capítulo 4

# Determinação do SIL Requerido

## 4.1 Introdução

Conforme discutido anteriormente, os valores de SIL refletem os níveis de confiabilidade que devem ser fornecidos pelos SIS, no que se refere à sua função principal, que é a de cumprir uma dada determinada função de segurança quando da ocorrência de um evento perigoso. Os níveis de SIL Requerido são fixados em função do nível de risco imposto pelo evento perigoso que gera a demanda pela atuação do SIS. Para a determinação deste valor de confiabilidade requerido, é necessário realizar uma análise de risco específica para a sua função de segurança.

O SIL adequado para o SIS é o que faz com que o risco inerente ao processo seja igual ou menor do que o nível do risco aceitável, proporcionando assim a segurança necessária para a operação da planta.

Existem várias maneiras de se determinar o SIL, mas nenhuma norma controla ou exige um procedimento específico, e esta atividade de determinação do SIL, passo essencial no projeto de controle do processo e do SIS, é fundamental, e passa sempre por uma avaliação com componentes subjetivos. Há países em que a legislação exige que se comprove matematicamente que o processo com seu SIS e outras camadas de proteção atingem o SIL desejado (BEGA et al. 2003).

Normas relacionadas ao assunto, como as apresentadas na seção 3.5, sugerem metodologias para a determinação do SIL a ser implementado pelo sistema de segurança. As seções a seguir apresentam, de forma bastante resumida, as principais metodologias

disponíveis na literatura para a determinação do SIL requerido.

## 4.2 Metodologias para a Determinação do SIL Requerido

A experiência tem mostrado que diferentes técnicas para avaliação do SIL requerido podem levar a resultados significativamente diferentes. As técnicas qualitativas podem resultar em respostas pessimistas (por exemplo, um nível super-estimado de SIL requerido). Esta dificuldade é gerada pela dificuldade de "calibrar" estas técnicas para os padrões de risco corporativos. Metodologias mais quantitativas (que podem ser mais facilmente calibradas para os critérios de risco corporativos) podem levar a resultados significativamente mais baixos (GRUHN 2004).

### 4.2.1 Metodologias Qualitativas e Semi-Qualitativas

Existem diversas metodologias para a determinação do SIL Requerido de um sistema de proteção e dos métodos disponíveis alguns são qualitativos e outros quantitativos ou semi-quantitativos.

É possível dizer que os métodos qualitativos são baseados na experiência e/ou aplicação de boas práticas de engenharia, além de serem de emprego rápido e direto, porém, dada estas características, não garantem maior repetibilidade. Basicamente utilizam uma matriz de risco ou gráfico de risco para chegar a um valor de SIL. O método conhecido como metodologia do gráfico de risco, é o mais comumente empregado desta categoria e tem como origem a norma alemã DIN VDE 19250 (DIN-VDE-19250 1998).

#### 4.2.1.1 Método da Matriz de Camada de Segurança

Um método qualitativo descrito pelas normas do IEC é denominada "Método da Matriz de Camada de Segurança", ou do inglês, *Safety Layer Matrix Method*. Esta metodologia está descrita no Anexo E da Parte 5 da IEC 61508 (IEC-61508-5 1998) e este mesmo procedimento está detalhado na Norma da ISA S.84.01, no Anexo A.3.1, onde é denominado "Matriz de Camada de Segurança", ou do inglês, *Safety Layer Matrix*. A origem deste método é atribuído à uma publicação do AICHE (AIChE 1993).

Os sistemas de segurança de plantas de processos industriais são compostos por vários subsistemas de segurança chamados barreiras de proteção, sendo que este número de subsistemas depende do grau de perigo que a planta oferece. A Norma IEC 61508 define algumas exigências básicas para que as camadas de proteção sejam consideradas nesta metodologia (para mais detalhes, ver (IEC-61508-5 1998)):

- Dispositivos de redução de risco SIS e não-SIS independentes;
- Cada dispositivo de redução de risco deve ser uma camada de proteção independente;
- Cada camada de proteção deve ser capaz de reduzir o SIL de 1 fator (isto é, um FRR de pelo menos 10).

O método então, determina o SIL para o SIS pela utilização da matriz apresentada na Figura 4.1:

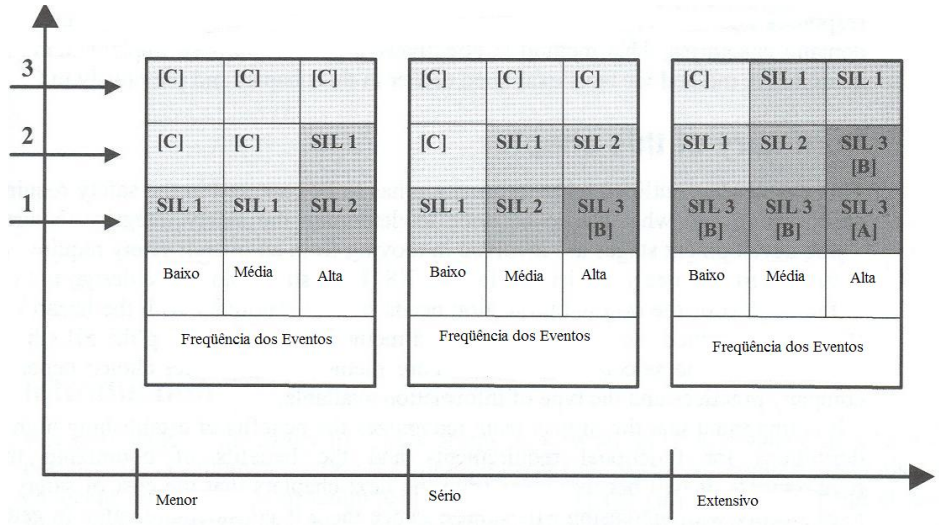


FIGURA 4.1: Matriz de Camada de Segurança

O eixo vertical apresenta o número de camadas de proteção independentes que protegem o processo, incluindo o SIS que está sendo analisado, enquanto que o eixo horizontal apresenta os critérios para severidade do impacto de eventos perigosos. As freqüências dos eventos perigosos são combinados com estes parâmetros e então determina-se o valor requerido de SIL.

Cabe ressaltar que, em relação aos resultados apresentados na Figura 4.1:

- "[C]" indica que não é requerido mais um fator de redução de risco;
- "SIL 3 [B]" indica que uma análise de risco/perigos é necessária para a determinação da necessidade de redução de risco adicional;
- 'SIL 3 [A]" indica que uma redução de risco é necessária.

As como principais características desta abordagem, é possível citar: método qualitativo e baseado em categorias; simples e de fácil aplicação; avalia o risco combinando a freqüência e a severidade do impacto de eventos perigosos; e depende da calibração da escala de severidade e da correta identificação das camadas de proteção válidas.

#### 4.2.1.2 Gráfico de Risco

O método conhecido como metodologia do gráfico de risco, tem como origem a norma alemã DIN VDE 19250 (DIN-VDE-19250 1998) e, originalmente expressa os níveis de classificação SIL em termos de classe AK-1 a AK-8. Os parâmetros considerados nesta avaliação são: a taxa de demanda do sistema de segurança (W); a conseqüência (C) caso o sistema de segurança não existisse ou não executasse sua função no momento de uma demanda; o fator de ocupação (F), que representa a probabilidade da área exposta ao evento perigoso estar ocupada; e a probabilidade de evitar o evento perigoso (P), que representa a probabilidade de que, dado que existam pessoas na área vulnerável ao evento perigoso, que as mesmas consigam evitar a exposição, no caso de falha na demanda do sistema de proteção. Após a seleção de cada um dos 4 parâmetros relacionados, utiliza-se o gráfico de risco apropriado para a leitura da combinação destes parâmetros e seleção do valor mínimo de redução de risco necessário para o sistema de segurança em análise (CHAME et al. 2007). A Figura 4.2 apresenta o gráfico de risco referenciado.

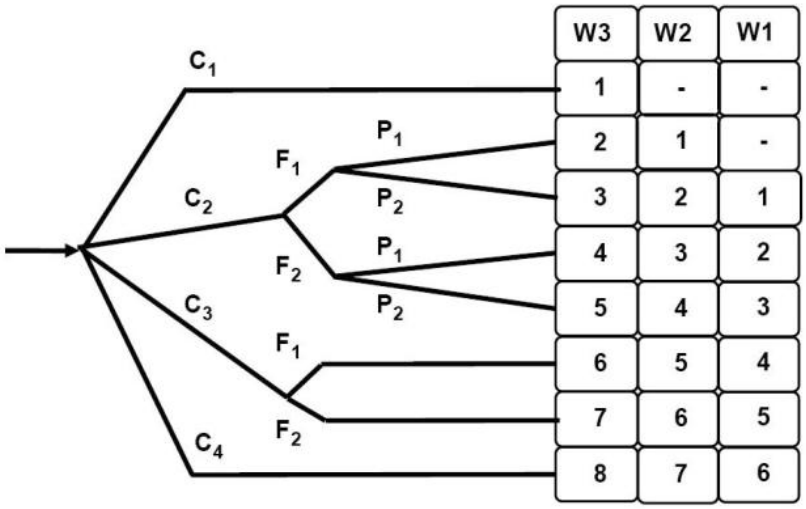


FIGURA 4.2: Gráfico de Risco - DIN V 19250

A Tabela 4.1 apresenta os parâmetros dos gráficos de risco citados acima.

TABELA 4.1: Parâmetros do Gráfico Risco

| | **Conseqûencia (C)** |
|---|---|
| C1 | Danos leves a pessoas |
| C2 | Danos sérios e permanentes a uma ou mais pessoas, morte de uma pessoa |
| C3 | Morte de várias pessoas |
| C4 | Efeitos Catastróficos, elevado número de mortes |
| | **Freqüência e Tempo de Exposição (F)** |
| F1 | Freqüência de exposição à zona de perigo de rara a freqüente |
| F2 | Freqüência de exposição à zona de perigo de freqüente a permanente |
| | **Possibilidade de evitar o evento perigoso (P)** |
| P1 | Possibilidade sobre certas condições |
| P2 | Quase Impossível |
| | **Probabilidade de Ocorrência (W)** |
| W1 | Probabilidade bem pequena de que eventos indesejados venham a ocorrer |
| W2 | Probabilidade pequena de que eventos indesejados venham a ocorrer |
| W3 | Probabilidade relativamente alta de que eventos indesejados venham a ocorrer |

As principais características desta abordagem são: metodologia qualitativa e baseada em categorias que incluem diretamente provisões para itens como ocupação e habilidade para escapar do evento perigoso; inicialmente desenvolvido para normas da indústria alemã e comumente utilizadas na União Européia; acurácia depende da interpretação das categorias. Para mais informações, esta metodologia está detalhada na parte 5 da Norma do IEC (IEC-61508-5 1998).

#### 4.2.1.3 Gráfico de Risco Calibrado

A calibração consiste na determinação de valores numéricos para parâmetros do gráfico de risco, de acordo com padrões de aceitabilidade de riscos existentes. Como principais objetivos da calibração, é possível citar: descrever todos os parâmetros de forma a permitir que o grupo de trabalho tome julgamentos objetivos baseados nas características da aplicação para a determinação do SIL; garantir que o SIL selecionado para a aplicação esteja de acordo com os critérios corporativos de risco e leve em consideração riscos provenientes de outras fontes; e permitir que o processo de seleção do parâmetro possa ser verificado.

A Figura 4.3 apresenta o gráfico de risco calibrado apresentado pela Norma IEC 61511 (IEC-61511 2003):

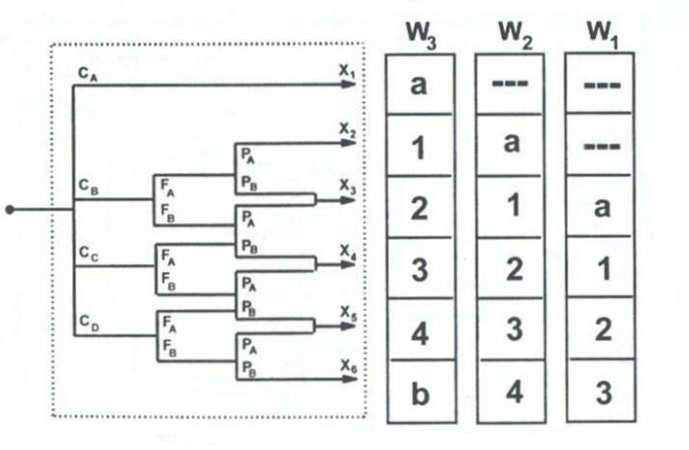


FIGURA 4.3: Gráfico de Risco Calibrado

A leitura do gráfico apresentado na Figura 4.3 se dá basicamente da mesma forma que o gráfico de risco apresentado na Figura 4.2. É possível citar como principais características desta abordagem: metodologia semi-qualitativa e baseada em categorias que incluem diretamente provisões para itens como ocupação e habilidade para escapar do evento perigoso; requer que a tabela de parâmetros e a utilização do Gráfico de Risco sejam validadas e os riscos para vida devem ser considerados sobre dois aspectos: Risco Individual (definido como o risco por ano do indivíduo mais exposto) e Risco Social (definido como o risco total por ano para um grupo de indivíduos expostos). Para mais informações, esta metodologia está detalhada na parte 5 da Norma do IEC (IEC-61508-5 1998).

### 4.2.2 Metodologias Quantitativas

Os métodos quantitativos utilizam modelos e expressões matemáticas para chegar a um valor de SIL, sendo, portanto mais objetivos e desde que sejam utilizados dados numéricos consistentes, garantem a repetibilidade da avaliação. A abordagem quantitativa é freqüentemente utilizada quando há interesse em se obter uma avaliação mais precisa e objetiva, o que tipicamente ocorre quando o método qualitativo indica um nível alto de SIL. Quantitativamente, o SIL é determinado pela diferença entre o nível de risco calculado para o processo, sem o sistema de proteção, e o nível de risco considerado tolerável pela empresa ou órgão responsável.

### 4.2.3 LOPA - *Layer of Protection Analysis*

A LOPA (do inglês, *Layers of Protection Analysis*) ou Análise de Camadas de Proteção é uma técnica de análise de risco desenvolvida para avaliar o risco de cenários de acidente considerando as camadas independentes de proteção pertinentes e determinar se existem camadas suficientes para proteção dos cenários de acidente em análise. A LOPA é uma técnica semi-quantitativa, situada entre técnicas puramente qualitativas como APP e HAZOP e a Análise Quantitativa de Riscos.

A técnica de LOPA foi desenvolvida pelo AIChE e apresentada originalmente em uma publicação de 1993. Consiste basicamente numa metodologia baseada na análise das camadas de proteção do sistema, ou seja, a segurança de uma instalação industrial é vista como em camadas concêntricas, cada uma delas recebendo um "peso" para a avaliação completa do sistema. Como vantagem, esta abordagem leva explicitamente em consideração fatores de redução de risco, tais como alarmes e válvula de alívio, que devem ser incorporados como ajustes na metodologia do gráfico de risco. A sua boa aceitação é função da facilidade de uso e precisão dos resultados, bem como da repetibilidade da avaliação.

Entre os objetivos principais para a utilização do LOPA está a possibilidade de responder a questões relativas ao número e eficiência das salvaguardas existentes, através de uma abordagem sistemática. Questões de subjetividade de classificação de cenários a que as técnicas qualitativas estão sujeitas são minimizadas nesta técnica.

Esta metodologia baseia-se na execução de seis etapas (AIChE 2001), definidas a

seguir:

- **Etapa 1**: Identificar critério para seleção de cenários;
- **Etapa 2**: Identificar o Cenário de Acidente a ser analisado, baseado em um par único de causa-conseqüência;
- **Etapa 3**: Identificar o(s) Evento(s) Iniciador(es) para o cenário em análise e determinar a freqüência do evento iniciador;
- **Etapa 4**: Identificar as Camadas Independentes de Proteção (CIPs), determinando quais salvaguardas são consideradas como CIPs e estimar a probabilidade de falha na demanda de cada camada independente de proteção;
- **Etapa 5**: Estimar o risco do cenário em análise, através da combinação de conseqüência e os dados da CIP;
- **Etapa 6**: Avaliar o risco do cenário de forma a tomada de decisão com relação à aceitabilidade do mesmo.

Conforme mencionado anteriormente, a LOPA avalia se existem camadas de proteção suficientes para evitar a ocorrência de um cenário de acidente e a eficiência destas proteções. Diversos tipos de camadas são considerados, conforme ilustrado na Figura 4.4 (AIChE 2001).

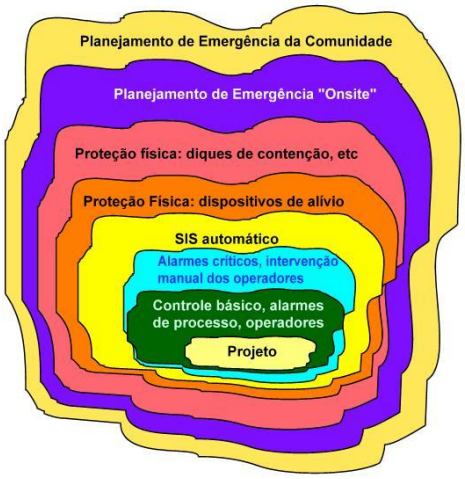


FIGURA 4.4: Camadas LOPA

Um determinado cenário pode necessitar de uma ou mais camadas, dependendo da complexidade do processo e da severidade potencial das conseqüências. Observa-se que para cada cenário analisado, o sucesso na atuação de qualquer uma das camadas deve ser obrigatoriamente suficiente para prevenir as conseqüências avaliadas. Porém, como nenhuma camada tem 100 % de probabilidade de sucesso, a utilização de diversas camadas pode ser necessária de forma a tornar o risco do cenário aceitável.

#### 4.2.3.1 Critérios para Seleção de Cenários e Avaliação das Conseqüências

Os cenários a serem analisados pela LOPA são formalmente aqueles identificados previamente em estudos qualitativos de identificação de perigos, APP/HAZOP, conforme a classificação de risco da Matriz de Aceitabilidade ou cenários identificados como relevantes para o sistema em análise, no caso de utilização da LOPA para a avaliação de níveis de integridade de segurança (SIL). Estes cenários devem ser definidos no mínimo pelos dois elementos abaixo:

- Uma causa que inicia a seqüência de eventos e;
- Uma conseqüência que irá ocorrer caso a seqüência de eventos continue sem interrupção.

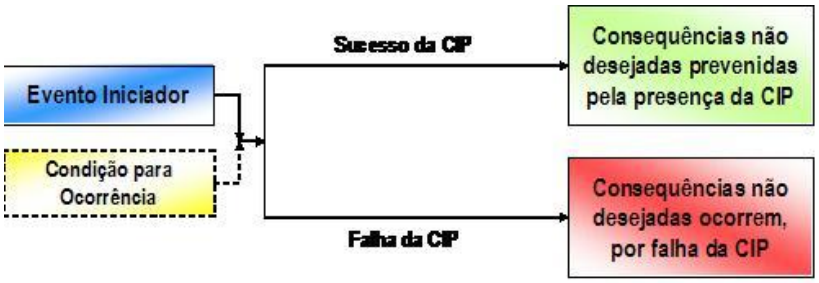


FIGURA 4.5: Sucesso e Falha LOPA

Caso um mesmo cenário dê origem a mais de uma conseqüência, diferentes cenários deverão ser considerados para a análise na LOPA. Adicionalmente, o cenário pode incluir ainda, conforme indicado na Figura 4.5:

- Condições ou eventos que devem ocorrer ou estar presentes para que o cenário se desenvolva (por exemplo, cenários que só ocorrem em determinada época do

ano ou número determinado de vezes ao ano, como operações de carregamento e descarregamento de navios);

- Falha das salvaguardas (CIPs ou não).

#### 4.2.3.2 Definição das CIPs e Análise da PFD das CIPs

Conforme mencionado anteriormente, toda CIP é uma salvaguarda, mas nem toda salvaguarda pode ser considerada uma CIP. Para que a proteção seja classificada como CIP, os seguintes critérios devem ser obedecidos:

- Ser eficiente: a CIP deve ser capaz de prevenir a ocorrência das conseqüências do cenário que está sendo analisado. A eficiência da camada deve ser quantificável, em termos da sua probabilidade de falha na demanda (PFD). Para ser considerada uma CIP, a sua PFD deve ser no máximo igual a 0,1, ou seja, deve proporcionar uma redução de riscos equivalente a pelo menos um fator de 10.

- Ser independente: a CIP deve ser independente em relação aos componentes de outras camadas de proteção associadas ao cenário em análise. Não deve existir também relação entre o evento iniciador e a habilidade da CIP em desempenhar sua função (por exemplo, se a causa do cenário for uma falha do sistema de controle, este não contará como CIP);

- Ser auditável: a camada deve ser auditável no sentido de demonstrar que atinge os requisitos para ser considerada uma CIP (eficiência e independência). A auditabilidade pode ser garantida através de documentação, revisão, teste ou outros meios.

Quanto à sua forma de atuação e quanto à sua eficiência em reduzir a freqüência ou as conseqüências do cenário, as salvaguardas podem ser classificadas em:

- Ativa ou Passiva

- Preventiva (antes da liberação) ou mitigatória (após a liberação).

Para a documentação da análise realizada, pode ser utilizado um formulário, conforme apresentado na Figura 4.6.

| Número do Cenário: | Descrição do Cenário: | Equipamento: | |
|---|---|---|---|
| Data: | Descrição | Probabilidade | Freqüência (/ano) |
| Critério de Aceitabilidade de Risco: | | | |
| Conseqüência: | | | |
| | Probabilidade de Ignição | | |
| | Fator de Presença | | |
| | Probabilidade de Fatalidades | | |
| Evento Iniciador: | | | |
| | Eventos Externos | | |
| | Falhas de Equipamentos | | |
| | Erros Humanos | | |
| Camadas de Proteção Independentes: | | | |
| | Dispositivo de Alívio | | |
| | Dique de Contenção | | |
| | Intervenção do Operador | | |
| PFD Total | | | |
| Critério de Aceitabilidade de Risco Atingido? (Sim/Não) | | | |
| Ações a serem tomadas caso o critério não tenha sido atingido: | | | |
| Observações: | | | |

FIGURA 4.6: Exemplo Planilha LOPA

# Capítulo 5

# Avaliação da PFD de Sistemas Instrumentados de Segurança

## 5.1 Introdução

Cálculos de confiabilidade são realizados por várias razões. Conforme apresentado anteriormente no Capítulo 2, uma importante medida de capacidade de redução de risco de uma Função Instrumentada de Segurança, FIS, é o atributo de confiabilidade PFD, ou Probabilidade de Falha na Demanda. A FIS deve ser projetada e configurada para atingir o SIL requerido pelo processo. Assim, a PFD para a FIS deve estar na faixa de valores especificada para o SIL exigido, conforme apresentado na Tabela 3.1. Se não estiver, será necessário reprojetar o SIL ou buscar outra alternativa que garanta o atendimento a este requisito. O valor da PFD para a FIS é obtido pela combinação das PFDs de todos os componentes do sistema.

Normas baseadas em performance, como ISA 84.01 e IEC 61508 (IEC-61508 1998) utilizam uma combinação de cálculos de confiabilidade de *hardware* para reduzir o efeito de falhas aleatórias e regras qualitativas para combater falhas sistemáticas. A etapa de verificação do *hardware* requer que sejam calculadas alguns parâmetros de segurança para o SIS, como a PFD e a SFF (do inglês, *Safe Failure Fraction*), atributo discutido na seção 3.7. Ambas as medidas têm que estar de acordo com as regras e as tabelas das normas para cada nível de redução de risco se a companhia quiser atender às referidas Normas (GOBLE & BEURDEN 2002).

Dado este cenário, este capítulo tem como objetivo discutir as diferentes alternativas para o cálculo da PFD de Funções Instrumentadas de Segurança e apresentar detalhadamente a técnica sugerida pela Parte 6 da Norma do IEC (IEC-61508-6 2000), incluindo a apresentação da metodologia proposta, a dedução das equações de cálculo da PFD, inclusive para uma configuração *koon* qualquer, bem como discutir a possibilidade de testes parciais de componentes do sistema de segurança analisado, o fator de diagnóstico de cobertura, a modelagem das falhas de causa comum e de testes imperfeitos.

## 5.2 Taxonomia e Terminologia da Norma IEC 61508

As principais variáveis utilizadas nas expressões matemáticas e abreviações presentes neste trabalho estão apresentadas na Tabela 5.1. Tanto quanto possível, foram mantidas precisamente a terminologia e representações das variáveis que aparecem nas expressões presentes na Parte 6 da IEC 61508 (IEC-61508-6 2000). A Figura 5.1 ilustra algumas destas relações consideradas na Norma.

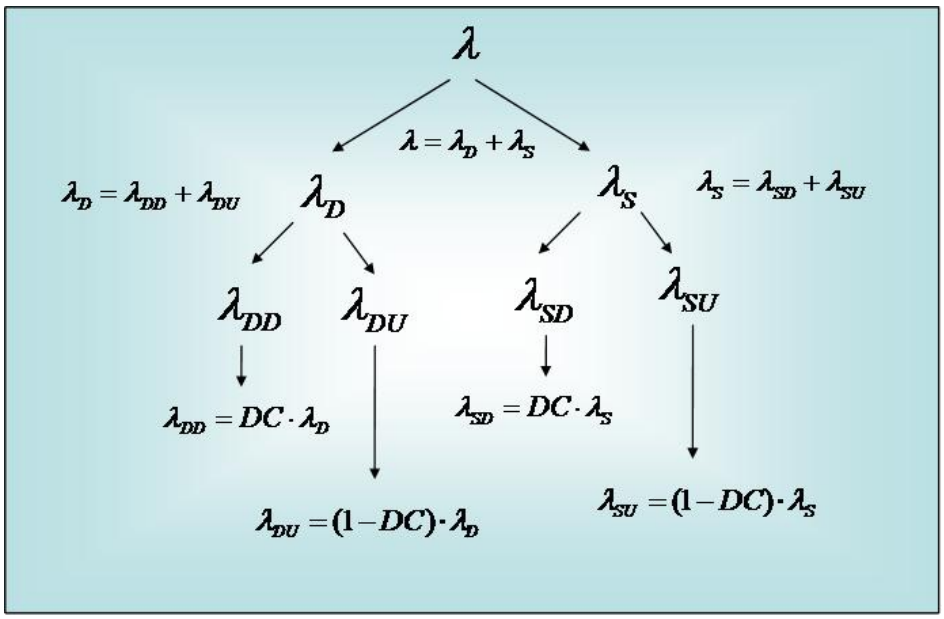


FIGURA 5.1: Relações - Norma IEC 61508

TABELA 5.1: Terminologia e Representações das Variáveis

| | |
|---|---|
| $t_{CE}$ | Tempo médio no estado falho equivalente de um canal relativo às configurações 1oo1, 1oo2, 2oo2, 2oo2, 1oo3 e 2oo3 |
| $t_{GE}$ | Tempo médio no estado falho equivalente para as configurações 1oo2 e 2oo3 |
| $t_{CE}^{'}$ | Tempo médio no estado falho equivalente de um canal relativo à configuração 1oo2D |
| $t_{GE}^{'}$ | Tempo médio no estado falho equivalente para a configuração 1oo2D |
| $\beta$ | Fator beta para falhas não-detectadas |
| $\beta_D$ | Fator beta para falhas detectadas |
| $\lambda$ | Taxa de falha total (taxa de falha crítica + taxa de falha segura) |
| $\lambda_D$ | Taxa de falha perigosa (*dangerous failure rate*) |
| $\lambda_{DD}$ | Taxa de falha detectada (*detected dangerous failure rate*) |
| $\lambda_{DU}$ | Taxa de falha não-detectada (*undetected dangerous failure rate*) |
| $\lambda_S$ | Taxa de falha segura (*safe failure rate*) |
| $\lambda_{SD}$ | Taxa de falha segura detectada (*detected safe failure rate*) |
| $\lambda_{SU}$ | Taxa de falha segura não-detectada (*undetected safe failure rate*) |

## 5.3 Alternativas para Cálculo da PFD de Sistemas Instrumentados de Segurança

Existem diversas técnicas disponíveis para a análise da integridade de segurança do *hardware* de sistemas de segurança E/E/EP (elétricos/eletrônicos e eletrônicos progamáveis), sendo duas das mais comuns as técnicas de diagramas de blocos de confiabilidade e a abordagem markoviana. Ambos os métodos, se devidamente aplicados, levam a resultados similares; no entanto, no caso de subsistemas eletrônicos programáveis complexos pode ocorrer uma perda de acurácia quando diagramas de bloco são utilizados comparados com a abordagem Markoviana. Entretanto, esta perda de acurácia pode não ser significativa no contexto do análise do sistema de segurança $E/E/EP$ completo e também nos casos onde a acurácia dos dados de confiabilidade utilizados na análise é levada em consideração. De qualquer forma, no caso de subsistemas eletrônicos programáveis complexos, a análise por diagramas de blocos de confiabilidade tende a apresentar resultados com valores mais pessimistas do nível de integridade de segurança do *hardware* do que os provenientes da abordagem markoviana, ou seja, diagramas de blocos de confiabilidade apresentam valores de PFD que tendem a ser ligeiramente superiores aos calculados pela abordagem markoviana.

A Norma IEC 61508 utiliza a técnica de modelagem por diagramas de blocos de confiabilidade. Um diagrama de bloco de confiabilidade é a representação gráfica da estrutura lógica do sistema em termos de subsistemas e componentes.

De acordo com a Norma IEC 61078, a técnica de Modelagem por Diagramas de Blocos de Confiabilidade tem como objetivo primário ser aplicada a sistemas não reparáveis e em sistemas onde a ordem de ocorrência das falhas não importa. Para sistemas onde as ordens das falhas são levadas em consideração ou onde reparos no sistema podem acontecer, outras técnicas de modelagem, como a abordagem markoviana, são mais apropriadas (IEC-61078 2006).

ALVARENGA (2005) cita que a modelagem por diagrama de blocos permite que os caminhos de sucesso do sistema sejam representados da forma com a qual os subsistemas e componentes estão logicamente conectados. Esta técnica é apropriada para modelar uma única função de um dado sistema. Se o sistema possui mais de uma função, cada função deve ser considerada individualmente, isto é, será necessária a construção de um diagrama de bloco para cada uma das funções.

Conforme destaca (OLIVEIRA n.d.), embora a modelagem através de diagrama de blocos algumas vezes coincida com o arranjo físico do sistema, este fato não deve ser considerado como uma regra geral; muito pelo contrário, na maioria das vezes este não é o caso. O diagrama de blocos é uma representação do arranjo lógico existente entre o funcionamento dos vários componentes, de forma a fornecer uma indicação dos vários modos de funcionamento do sistema.

A Norma da ISA (ANSI/ISA-84.00.01 2004) descreve três métodos para modelagem do sistema de segurança e verificação do seu respectivo SIL. São eles: (a) Equações simplificadas, (b) Árvore de Falhas e (c) Abordagem Markoviana. O termo "equações simplificadas" é de alguma forma mal compreendido; elas são equações algébricas relativamente simples, mas são derivadas de complexos modelos de Markov. O relatório técnico da ISA modela o mesmo sistema (sensores redundantes, lógica e elementos finais) utilizando todas as três técnicas. Os resultados (em termos de falhas seguras e falhas perigosas) são estatisticamente o mesmo (GRUHN 2002).

A técnica de avaliação por árvore de falhas para avaliação quantitativa de parâmetros de confiabilidade é baseada em uma investigação das causas de um determinado fato, ou seja, a construção de uma árvore de falhas consiste em um processo lógico que,

partindo de um evento indesejado (normalmente, falha do sistema), busca todas as combinações de falhas dos componentes que levam à ocorrência de tal evento.

Dentre os métodos utilizados no cálculo de atributos de confiabilidade, o markoviano é um dos mais poderosos. Ele modela o sistema em evidência por intermédio dos estados internos que o sistema pode assumir e as respectivas transições entre eles (DINIZ 1997).

Conforme cita DROGUETT (2002), a Análise Markoviana constitui-se em uma poderosa e flexível técnica de modelagem e análise amplamente empregada em análises dinâmicas de confiabilidade e disponibilidade de sistemas. O comportamento da confiabilidade de um sistema é representado usando-se um diagrama de transições entre estados, o qual consiste em um conjunto de estados discretos nos quais o sistema pode se encontrar em um determinado momento, e define as taxas segundo as quais transições entre esses estados podem ocorrer. Desta forma, modelos markovianos consistem em representações de cadeias de eventos, ou seja, transições dentro do sistema que, no contexto da análise de confiabilidade e disponibilidade, correspondem a seqüências de falhas e reparos.

## 5.4 Representação da PFD como produto de uma freqüência média por uma duração média

De um modo geral, a PFD de um sistema de proteção qualquer pode ser expressa como o produto da freqüência média de ocorrência do estado falho pela duração média da permanência neste estado, ou seja:

$$PFD = \phi \cdot T \tag{5.1}$$

onde $\phi$ é a freqüência média de ocorrência de uma falha crítica do sistema em um dado período de tempo e $T$ é o tempo médio de permanência neste estado.

Tipicamente para um sistema de proteção, o período de tempo de interesse é aquele compreendido entre dois testes consecutivos do sistema, ou seja, o intervalo entre testes periódicos, aqui denominado $T_1$ para seguir a mesma nomenclatura da Norma IEC 61508 (IEC-61508 1998), base deste trabalho. Tomando o período $T_1$ como base, então a freqüência média de falhas críticas no período pode ser expressa por:

$$\phi = \frac{1}{T_1} \int_0^{T_1} \lambda(t)\, dt \tag{5.2}$$

onde $\lambda(t)$ é a taxa de falha instantânea do sistema de proteção, dada pela relação entre a densidade de probabilidade de falhas críticas, $f(t)$, e a confiabilidade do sistema, $R(t)$ (ver equação 5.3), ou alternativamente, com a sua não-confiabilidade F(t)=1-R(t), (OLIVEIRA n.d.).

$$\lambda(t) = \frac{f(t)}{R(t)} = \frac{f(t)}{1 - F(t)} \cong f(t) \tag{5.3}$$

A aproximação apresentada na equação 5.3 acima, é válida somente para a condição de que o produto $\lambda(t) \cdot T_1$ seja muito menor que 1, pois sendo esta afirmação verdadeira, é possível aproximar a distribuição exponencial (ver equação 5.4) por seus dois primeiros termos, conforme apresentado a seguir:

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots \Rightarrow \quad e^x \cong 1 + x \tag{5.4}$$

ou seja, para o caso da função de confiabilidade, $R(t) = e^{-\lambda t}$ (vide equação 2.20), temos:

$$e^{-\lambda t} = 1 - \lambda t + \frac{(-\lambda t)^2}{2!} - \frac{(-\lambda t)^3}{3!} + \ldots \Rightarrow \quad e^{-\lambda t} \cong 1 - \lambda t \tag{5.5}$$

resultado para $\lambda t << 1$ e que valida a aproximação apresentada na equação 5.3.

Seja uma variável aleatória qualquer $X$. É sabido que o valor médio (ou valor esperado) de uma variável aleatória com densidade de probabilidade $f(x)$ em um intervalo $[0, T_1]$ pode ser dada pela equação 5.6:

$$E(X) = \frac{\int_0^x (x) f(x)\, dx}{\int_0^x f(x)\, dx} \tag{5.6}$$

Assumindo agora a variável aleatória $X$ como sendo a variável aleatória "tempo no estado falho", no intervalo $[0, T_1]$ (ver Figura 5.2), pode-se dizer que esta variável representa o tempo compreendido entre o momento em que a falha ocorre (t) e o tempo ($T_1$) e que está sendo considerando que esta falha é não detectada, e que portanto, permanece no estado falho até o instante $T_1$, quando ocorrerá seu reparo ou sua substituição.

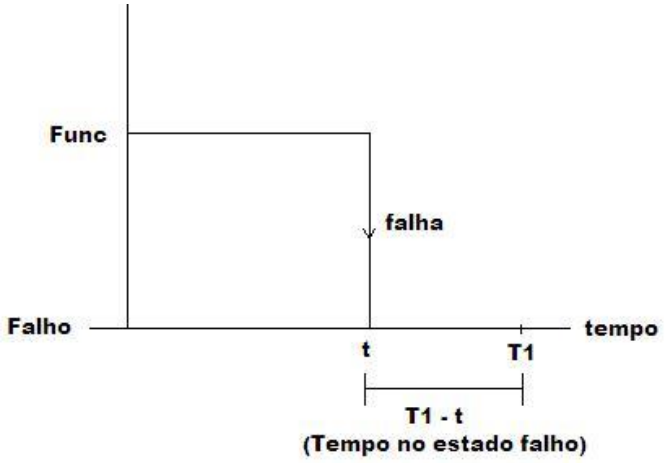


FIGURA 5.2: Representação do Tempo no Estado Falho

Por sua vez, considerando a equação 5.6, é possível calcular a duração média $T$ de permanência no estado falho pela equação 5.7, onde $f(t)$ é a função de densidade de probabilidade de falha do sistema:

$$T = E\left(T_1 - t\right) = \frac{\int_0^{T_1} (T_1 - t) f(t)\, dt}{\int_0^{T_1} f(t)\, dt} \tag{5.7}$$

Este enfoque é o adotado na Parte 6 da IEC 61508, onde são apresentadas expressões para se avaliar a PFD das arquiteturas mais comuns para os SISs da indústria em geral.

Considerando o apresentado nas equações 2.18, 2.20 e 2.4 e aplicando o discutido acima, considere-se um sistema de proteção de um único canal, ou seja, um sistema do tipo 1oo1, com taxa de falha crítica não-detectada (*dangerous undetected*) constante, $\lambda_{DU}$. A função de densidade de probabilidade pode ser escrita como $f(t) = \lambda_{DU} \cdot e^{-\lambda_{DU} t}$ (OLIVEIRA n.d.) pois, conforme apresentado na equação 2.4 e sabendo que $F(t) = 1 - R(t)$, pode-se deduzir:

$$f(t) = \frac{d[1 - R(t)]}{dt} = -\frac{dR(t)}{dt} = -\frac{d[e^{\lambda_{DU} t}]}{dt} \quad \Rightarrow \quad f(t) = \lambda_{DU} \cdot e^{-\lambda_{DU} t} \tag{5.8}$$

Dado o valor da densidade de probabilidade $f(t)$, podemos usar a equação 5.7 para calcular a duração média de permanência no estado falho para este sistema de um único canal, $T_{sistema}$, ou seja:

$$T_{sistema} = \frac{\int_0^{T_1} (T_1 - t)\lambda_{DU} \cdot e^{-\lambda_{DU} T_1}\, dt}{\int_0^{T_1} \lambda_{DU} \cdot e^{-\lambda_{DU} T_1}\, dt} \tag{5.9}$$

Resolvendo a equação 5.9, admitindo que $\lambda_{DU} T_1 << 1$, conforme discutido anteriormente, temos que:

$$T_{sistema} = \frac{T_1}{2} \tag{5.10}$$

e sabendo que a freqüência média de ocorrência de uma falha crítica do sistema em questão, $\phi_{sistema}$, no período de tempo considerado acima, é:

$$\phi_{sistema} = \lambda_{DU} \tag{5.11}$$

é possível verificar que substituindo-se as expressões 5.10 e 5.11 na equação 5.1, obtém-se:

$$PFD_{sistema} = \lambda_{DU} \cdot \frac{T_1}{2} \tag{5.12}$$

Nas equações acima, foi considerada apenas a contribuição das falhas não-detectadas durante o período entre testes. No entanto, considerando que o canal pode também ficar indisponível para reparo (por um período médio igual ao seu MTTR, *Mean Time to Repair* ou Tempo Médio de Reparo) caso o teste detecte uma falha do canal, então deve-se adicionar o MTTR à expressão de $T_{Sistema}$ dada na equação 5.10, de modo que a mesma deve ser reescrita como:

$$T_{sistema} = \frac{T_1}{2} + MTTR \tag{5.13}$$

Assim, a equação 5.12 torna-se:

$$PFD_{sistema} = \lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) \tag{5.14}$$

Adicionando-se a isto, a consideração de que, por conta da sua capacidade de auto-diagnóstico, o canal pode também ter uma taxa de falha crítica detectada (*dangerous detected*), $\lambda_{DD}$, a qual pode contribuir para a PFD do canal (caso o seu reparo seja feito com a planta em operação), então a equação da PFD torna-se:

$$PFD_{sistema} = \lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) + \lambda_{DD}MTTR \tag{5.15}$$

Para se reescrever a equação da PFD como o produto de uma freqüência por uma duração (como na equação 5.1), basta multiplicar e dividir a equação 5.15 por $\lambda_D = \lambda_{DU} + \lambda_{DD}$, chegando-se a:

$$PFD_{sistema} = \lambda_D \cdot t_{CE} \tag{5.16}$$

onde:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \tag{5.17}$$

Cabe destacar que $t_{CE}$ é o termo utilizado na Norma IEC 61508, para representar o tempo médio equivalente de permanência de um canal no estado de falha crítica (*channel equivalent mean downtime*, de acordo com a nomenclatura da Norma IEC 61508).

## 5.5 Metodologia de Cálculo da PFD apresentada na Norma IEC 61508

Cabe destacar, antes da apresentação da seção a seguir, que o Anexo B da Parte 6 da Norma IEC 61508 lista uma série de premissas consideradas para os cálculos das PFDs que serão apresentadas adiante neste trabalho e que devem ser consultadas no caso de utilização das mesmas para uma análise.

### 5.5.1 O Cálculo da PFD de um SIS de acordo com a Norma IEC 61508

Conforme já citado na Seção 3.5, a Norma IEC 61508 considera dois possíveis modos de operação para o sistema instrumentado de segurança (SIS): modo de operação de baixa demanda e o modo de operação de alta demanda. No modo de operação de baixa demanda considera-se que a freqüência de demanda para operação do SIS não é maior

do que uma por ano e também não maior do que duas vezes a freqüência de testes do sistema. O modo de operação de alta demanda ou modo contínuo considera que a freqüência de demanda para a operação do SIS é maior do que uma por ano e maior do que duas vezes o intervalo entre testes do sistema.

As unidades métricas que expressam os valores de SIL para cada um dos modos de operação do SIS são diferentes. Para o caso do modo de operação de baixa demanda, este valor é expresso em termos de probabilidade média de falha em funcionar conforme projetado na demanda, ou seja, a PFD. Para a outra possibilidade, modo de operação contínuo, este valor é expresso em taxa de falhas perigosas por ano. Ainda em função deste raciocínio, cada valor de SIL pode ser expresso em termos de PFD ou em taxa de falhas perigosas, conforme apresentado anteriormente na seção 3.4, em função do modo de operação do sistema de segurança em análise. Desta forma, é preciso ressaltar que para cada caso, existe um diferente tipo de cálculo para se determinar se o SIL requerido é atendido ou não.

Dado que para sistemas instrumentados de segurança (SIS) em indústrias de processo, o modo de operação característico do sistema de segurança é o de baixa demanda, é apresentado a seguir o procedimento para o cálculo da PFD sugerido na Norma IEC 61508 (IEC-61508-6 2000) para este caso.

As malhas de segurança que implementam uma função instrumentada de segurança são compostas pelos iniciadores da função, pelo executor da lógica e pelos atuadores. Analisando as falhas aleatórias de *hardware*, a PFD é matematicamente estimada através da soma das probabilidades de falha de cada um destes componentes, ou seja (MARSZAL & MITCHELL 2003):

1. Dispositivo de entrada da FIS (iniciador) falha em avisar ao executor da lógica para interromper o processo no momento de um evento perigoso;

2. Dispositivo executor da lógica falha em interromper o processo quando é avisado para tomar esta ação;

3. Dispositivo final de controle (atuador) falha em interromper o processo quando é comandado a tomar esta ação pelo executor da lógica.

Conforme citado, as malhas de segurança que implementam uma função instru-

mentada de segurança são compostas pelos iniciadores da função, pelo executor da lógica e pelos atuadores. A probabilidade de falha na demanda (PFD) média de uma função de segurança para um sistema de segurança (*safety-related system*) E/E/PE é determinada pelo cálculo e combinação da probabilidade de falha na demanda média de todos os subsistemas que em conjunto, provêm a função de segurança, ou seja:

$$PFD_{sistema} = PFD_I + PFD_L + PFD_A \tag{5.18}$$

onde:

- $PFD_{sistema}$ = Probabilidade de Falha na Demanda média da função de segurança;
- $PFD_I$ = Probabilidade de Falha na Demanda média do(s)iniciador(es) da função de segurança;
- $PFD_L$ = Probabilidade de Falha na Demanda média do executor da lógica da função de segurança;
- $PFD_A$ = Probabilidade de Falha na Demanda média do(s) atuador(es) da função de segurança;

Diagramas de bloco de confiabilidade são a representação gráfica da estrutura lógica de um sistema em termos de subsistemas e componentes. Estes blocos são arrumados para representar quais componentes são requeridos para o sucesso da operação. Probabilidades de sucesso da operação de componentes são combinados com o objetivo de calcular probabilidades de sucesso de operação do sistema. Este método é utilizado com a maior freqüência para avaliar a disponibilidade/indisponibilidade ou confiabilidade/não confiabilidade de sistemas. Desta forma, o sistema acima em termos de diagrama de blocos, seria representado como mostrado na Figura 5.3:


FIGURA 5.3: Diagrama de Blocos do Sistema

De acordo com a Norma IEC 61508 (IEC-61508-6 2000), para determinar a probabilidade de falha na demanda média para cada um dos subsistemas, o procedimento

sugerido consiste em desenhar o diagrama de bloco destacando os componentes do subsistema do elemento iniciador (sensor), os componentes do subsistema do executor da lógica e os componentes do subsistema do elemento final, ou seja, representar cada subsistema como um ou mais 1oo1, 1oo2, 2oo2, 1oo2D ou 2oo3 grupos de votação.

Em seguida, deve-se identificar e/ou calcular os demais parâmetros necessários para a determinação da PFD média do sistema em questão, sendo estes:

- Intervalo entre Testes;
- MTTR.

E para cada grupo de votação no subsistema (FLEMING 1975):

- Arquitetura;
- Cobertura de Diagnóstico de cada canal;
- Taxa de Falhas (por hora) de cada canal;
- Fator de Falha Comum para a interação entre os canais no grupo de votação.

Cabe destacar que é assumido que todo canal no grupo votado tem a mesma cobertura de diagnóstico e taxa de falha.

Desta forma, se a função de segurança depende de mais de um grupo de votação de sensores ou atuadores, a probabilidade de falha na demanda média do sensor ou do elemento final do subsistema deve ser calculada levando em consideração estas arquiteturas.

## 5.6 Dedução das Fórmulas de Cálculo da PFD apresentadas na Norma IEC 61508

Arquiteturas são configurações específicas de elementos de *hardware* e *software* num sistema. O Anexo B da Parte 6 da Norma IEC 61508, apresenta os cálculos da Probabilidade de Falha na Demanda, PFD, para algumas arquiteturas típicas de sistemas de segurança. São elas: 1oo1, 1oo2, 2oo2, 1oo2D e 2oo3, e as mesmas estão descritas e apresentadas a seguir.

### 5.6.1 Arquitetura 1oo1

Esta arquitetura consiste de um canal único, onde qualquer falha perigosa leva o sistema à falha da função de segurança quando uma demanda acontece. As Figuras 5.4 e 5.5, ilustram, respectivamente, o diagrama de bloco físico de um sistema 1oo1 e o diagrama de blocos de confiabilidade para o sistema 1oo1.

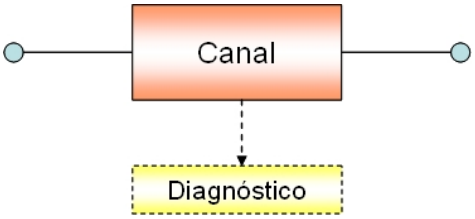


FIGURA 5.4: Diagrama de Blocos - Arranjo Físico - Arquitetura 1oo1

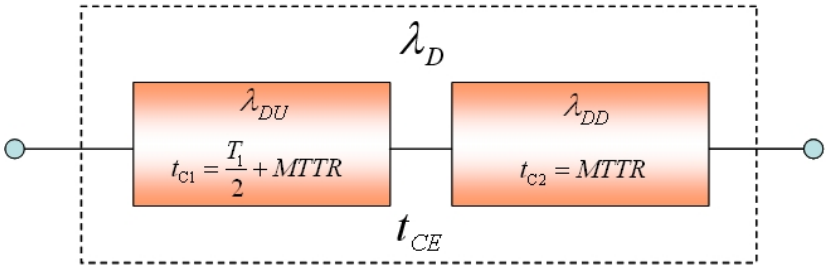


FIGURA 5.5: Diagrama de Bloco de Confiabilidade - Arquitetura 1oo1

Considerando que o canal (o único componente) também tem um modo falha perigoso e detectado, (do inglês, *dangerous detected*), $\lambda_{DD}$, ao qual está associado o mesmo tempo médio de restauração, MTTR, então, conforme visto na seção 5.4, a PFD pode ser escrita em termos de uma freqüência multiplicado por um intervalo de tempo:

$$PFD_{1oo1} = \phi \cdot T \tag{5.19}$$

onde $\phi$ é a freqüência, então, em termos da taxonomia da Norma IEC 61508 (ver Tabela 5.1):

$$PFD_{1oo1} = \lambda_D \cdot t_{CE} \tag{5.20}$$

onde $\lambda_D$ é a taxa de falhas perigosas para o canal, $\lambda_D = \lambda_{DU} + \lambda_{DD}$, e $t_{CE}$ é definido como um "tempo médio no estado falho equivalente" para o canal. Na realidade, a PFD corresponde à soma das contribuições dos modos de falha "não-detectado" e "detectado", ou seja:

$$PFD_{1oo1} = \lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) + \lambda_{DD}MTTR \tag{5.21}$$

e igualando as equações 5.20 e 5.21:

$$PFD_{1oo1} = \lambda_D \cdot t_{CE} = \lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) + \lambda_{DD}MTTR \tag{5.22}$$

chega-se a:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR \tag{5.23}$$

que é a equação apresentada na Norma IEC 61508 (IEC-61508 1998) para o $t_{CE}$ desta arquitetura, sendo então as equações 5.20 e 5.23 as equações que definem a PFD para um sistema com arquitetura 1oo1.

### 5.6.2 Arquitetura 1oo2

Esta arquitetura consiste de dois canais conectados em paralelo de tal forma que qualquer um dos canais pode processar a função de segurança. Desta forma, deve haver uma falha perigosa em ambos os canais antes que uma função de segurança falhe na demanda. É assumido que qualquer teste de diagnóstico somente reportará as falhas encontradas e não irão alterar qualquer estado de saída ou mudança na votação de saída, gerando apenas um alarme. As Figuras 5.6 e 5.7 apresentam os diagramas de blocos que representam o sistema, sendo o primeiro o que representa fisicamente o sistema e o segundo, a sua confiabilidade.

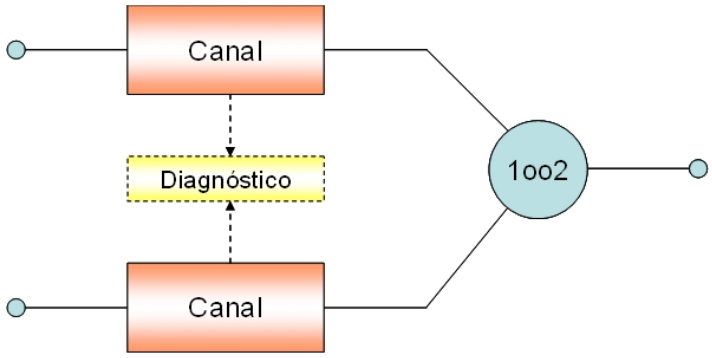


FIGURA 5.6: Diagrama de Blocos - Arranjo Físico - Arquitetura 1oo2

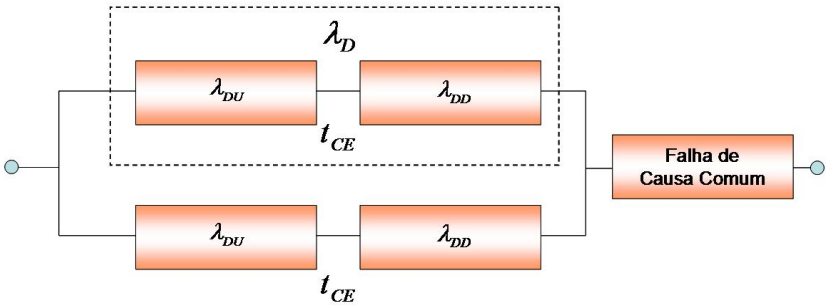


FIGURA 5.7: Diagrama de Blocos de Confiabilidade - Arquitetura 1oo2

Seguindo a mesma sistemática usada para um sistema com uma arquitetura 1oo1, a probabilidade de falha na demanda, PFD, pode ser escrita como o produto da freqüência de eventos de falha do sistema 1oo2 por uma duração média equivalente da falha do sistema, ou seja:

$$PFD_{1oo2} = \phi_{1oo2} \cdot T_{1oo2} \tag{5.24}$$

A freqüência $\phi_{1oo2}$ é o valor esperado (média do número de falhas do sistema no intervalo $[0,T_1]$). Para o sistema 1oo2, esse número corresponde ao número de vezes em que os dois canais entram no estado falho, ou mais especificamente, ao número de vezes em que o canal passa para o estado falho quando o outro já se encontra neste estado, enquanto que a duração $T_{1oo2}$ é o valor esperado (médio) do tempo em que o sistema 1oo2 permanece no estado falho durante o intervalo $[0,T_1]$.

Para a avaliação da freqüência $\phi_{1oo2}$, temos que, conforme apresentado anteriormente através da equação 5.3, a taxa de falha equivalente de um sistema qualquer é dada por:

$$\lambda_{sist}(t) = \frac{f(t)}{R(t)} = \frac{\frac{-dR(t)}{dT}}{R(t)} \tag{5.25}$$

Sabendo que a confiabilidade de um sistema de arquitetura 1oo2 pode ser escrita como:

$$R_{1oo2}(t) = e^{-\lambda_1 t} + e^{-\lambda_2 t} - e^{-(\lambda_1+\lambda_2)t} \tag{5.26}$$

e admitindo que $\lambda_1 = \lambda_2 = \lambda$ (taxa de falha do canal), então:

$$R_{1oo2}(t) = 2e^{-\lambda t} - e^{-2\lambda t} \tag{5.27}$$

fazendo as aproximações:

$$e^{-\lambda t} \cong 1 - \lambda t + \frac{(\lambda t)^2}{2} \tag{5.28}$$

$$e^{-2\lambda t} \cong 1 - 2\lambda t + \frac{(2\lambda t)^2}{2} \tag{5.29}$$

temos que:

$$R_{1oo2}(t) = 2 - 2\lambda t + (\lambda t)^2 - 1 + 2\lambda t - 2(\lambda t)^2$$

que resulta em:

$$R_{1oo2}(t) = 1 - \lambda^2 t^2 \tag{5.30}$$

Conforme indicado anteriormente na equação 5.25, a partir da densidade de probabilidade é possível obter:

$$f_{1oo2}(t) = 2\lambda^2 t \tag{5.31}$$

Portanto, da equação 5.25, obtém-se:

$$\lambda_{1oo2}(t) = \frac{2\lambda^2 t}{1 - \lambda^2 t^2} \tag{5.32}$$

que para um valor de $\lambda t << 1$, se reduz a:

$$\lambda_{1oo2}(t) \cong 2\lambda^2 t \tag{5.33}$$

A freqüência média de falhas no período [0,$T_1$] pode ser obtida, conforme a equação 5.2, da seguinte forma:

$$\phi_{1oo2} \quad = \quad \tfrac{1}{T_1}\int_0^{T_1} \lambda_{1oo2}(t)dt \quad = \quad \tfrac{1}{T_1}\int_0^{T_1} 2\lambda^2 t dt$$

que resulta em:

$$\phi_{1oo2} = \frac{1}{T_1}\cdot 2\lambda^2 \cdot \frac{T_1^2}{2} = \underbrace{\lambda^2 T_1}_{\lambda=\lambda_D} \quad \text{(taxa de falha total do canal)} \tag{5.34}$$

Para a avaliação de $T_{1oo2}$, analogamente ao caso de um canal (1oo1), $T_{1oo2}$ corresponde ao valor médio do tempo que o sistema 1oo2 permanece no estado falho, o qual pode ser calculado pela equação 5.7, substituindo-se a $f(t)$ do sistema 1oo2 dada pela equação 5.32. Assim, é possível obter:

$$T_{1oo2} = \frac{\int_0^{T_1}(T_1 - t)\cdot 2\lambda^2 t dt}{\int_0^{T_1} 2\lambda^2 t dt} = \frac{T_1}{3} \tag{5.35}$$

Analogamente ao caso do sistema 1oo1, existem ainda duas outras contribuições para o "tempo no estado falho" (*downtime*), que são o reparo após o teste e o reparo após uma falha detectada. No presente caso, 1oo2, essas contribuições envolvem as falhas dos dois canais. Assim:

$$T_{1oo2} = t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR)\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \tag{5.36}$$

onde:

- $\frac{\lambda_{DU}}{\lambda_D}$ = fração da taxa de falhas que acarreta um "tempo médio no estado falho", igual a $\left(\frac{T_1}{3} + MTTR\right)$;
- $\frac{\lambda_{DD}}{\lambda_D}$ = fração da $\lambda_D$ que acarreta um "tempo médio no estado falho", igual a MTTR.

Em função de tudo que foi descrito acima, é possível então calcular a PFD para um sistema com arquitetura 1oo2. Dado o apresentado na equação 5.24 e substituindo os resultados apresentados nas equações 5.34 e 5.35, temos:

$$PFD_{1oo2} = \lambda_D^2 T_1 T_{1oo2} \tag{5.37}$$

Da equação 5.17 pode-se ver que o "tempo médio no estado falho" para um canal pode ser aproximado por $T_1/2$, pois tipicamente $T_1 >> MTTR$ (embora nem sempre seja o caso). Portanto, escrevendo $t_{CE} \cong T_1/2$, ou seja, $T_1 \cong 2t_{CE}$ e substituindo na equação 5.37, chega-se a:

$$PFD_{1oo2} = 2\lambda_D^2 t_{CE} T_{1oo2} \tag{5.38}$$

Na nomenclatura da Norma IEC 61508, $T_{1oo2} = t_{GE}$, portanto:

$$PFD_{1oo2} = 2\lambda_D^2 t_{CE} t_{GE} \tag{5.39}$$

que é a equação apresentada na Norma IEC 61508 (IEC-61508 1998) para a PFD desta arquitetura.

### 5.6.3 Arquitetura 1oo2D

Esta arquitetura consiste em dois canais conectados em paralelo. Durante a operação normal, ambos os canais precisam demandar a função de segurança antes dela atuar. Além disso, se o teste de diagnóstico detectar uma falha em algum dos canais então a votação de saída é adaptada para que o estado de saída final siga o dado pelo outro canal. Se o teste de diagnóstico encontrar falhas em ambos os canais ou identificar uma discrepância que não pode ser alocada para algum dos canais, então a saída vai para a posição segura. De forma a detectar uma discrepância entre os canais, qualquer um dos canais pode determinar o estado do outro canal via caminhos independentes do outro canal.

A letra "D" significa "diagnóstico". Esta configuração é semelhante a uma configuração 1oo2 no sentido de que basta que um único canal responda corretamente a uma demanda para que a função de segurança seja executada. Assim, do ponto de vista

da segurança, esta configuração é igual à configuração 1oo2. A diferença está em que uma "falha detectada" ou segura, não causa a ativação da função de segurança, pois a partir do diagnóstico da falha de um canal, o sistema é reconfigurado para atuar como 1oo1, utilizando o canal remanescente (o qual supostamente estaria bem, exceto pela possibilidade de já haver sofrido uma falha não detectada). Portanto, a configuração 1oo2D provê praticamente o mesmo nível de segurança da 1oo2, mas apresenta uma menor freqüência de atuações espúrias da função de segurança. Neste aspecto, é semelhante a uma configuração 2oo3, pois somente duas falhas detectadas (uma em cada canal) causarão uma atuação espúria da função de segurança.

Conforme indicado na Norma IEC 61508, neste caso considera-se o efeito da "falha de segurança" (falha espúria, $\lambda_{SD}$), a qual também requer um tempo de restauração (MTTR). Todas as outras considerações para a avaliação da PFD são iguais às da arquitetura 1oo2, pois a diferença entre as duas reside no tratamento das falhas detectadas, como indicado no parágrafo anterior.

Conforme reafirmam LIMA & SAITO (2002), a diferença para a votação 1oo2 é que o diagnóstico de falha de um dos instrumentos degrada o esquema de votação para 1oo1. Caso o diagnóstico de falha seja nos dois instrumentos, a saída é modificada para um estado seguro.

É interessante notar na Figura 5.8, que a taxa de falhas detectada é considerada em apenas um dos canais. Isto significa que quando uma falha é detectada em um dos canais, o sistema reconfigura-se para funcionar como 1oo1 usando o canal remanescente, mas se uma segunda falha é detectada (agora no canal remanescente) o sistema comanda o desligamento seguro da planta. Dessa forma, duas falhas detectadas (uma em cada canal) não contribuem para a PFD do sistema.

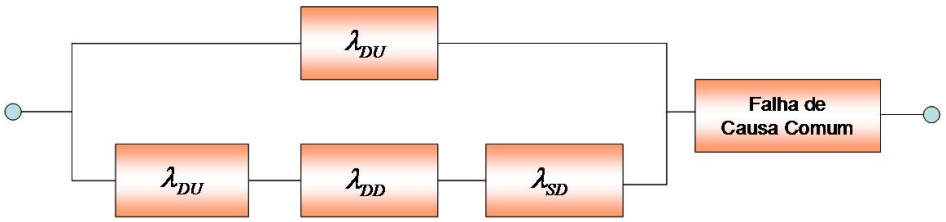


FIGURA 5.8: Arquitetura 1oo2D - IEC

Conforme GRUHN (2002), estes sistemas 1oo2D não são do tipo com votação 1oo2, onde se precisa de apenas um canal bom para iniciar o *shutdown*, ou *hot-back-up*,

onde apenas um canal está ativo, enquanto o outro assume em caso de falha do que estava ativo. Esta terminologia foi empregada pela primeira vez por Bill Goble em 1992, em seu livro da ISA "*Evaluating Control System Reliability*". Estes sistemas exigem ao menos duas falhas seguras simultâneas (por exemplo, falha desenergizando) para derrubar a unidade sem necessidade, e duas falhas perigosas simultâneas (por exemplo, travada em posição energizada) para uma falha do tipo não desliga em caso de necessidade.

No caso do sistema 1oo2, a PFD é dada pela equação 5.39. Para o caso do 1oo2D, a expressão é a mesma, exceto que um dos canais tem apenas o modo de falha perigoso não detectado, ou *dangerous undetected - DU*, e o outro tem os três modos de falha: DU, DD e SD. Daí pode-se escrever (sem incluir as Falhas de Causa Comum - FCCs):

$$PFD_{1oo2D} = 2\lambda_{DU}(\lambda_{DU} + \lambda_{DD} + \lambda_{SD})t'_{CE}t'_{GE} \tag{5.40}$$

onde:

$$t'_{CE} = \frac{\lambda_{DU}}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD} + \lambda_{SD}}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}}MTTR \tag{5.41}$$

e,

$$t'_{GE} = \frac{\lambda_{DU}}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DD} + \lambda_{SD}}{\lambda_{DU} + \lambda_{DD} + \lambda_{SD}}MTTR \tag{5.42}$$

### 5.6.4 Arquitetura 2oo2

Esta arquitetura consiste de dois canais conectados em paralelo de tal forma que ambos os canais precisam demandar a função de segurança antes que ela atue. Assume-se que qualquer teste de diagnóstico pode reportar somente as falhas encontradas e não mudar qualquer estado ou qualquer votação de saída. Qualquer diagnóstico de falha em um dos instrumentos apenas gera um alarme. As Figuras 5.9 e 5.10 apresentam os diagramas de bloco relevantes para esta arquitetura.

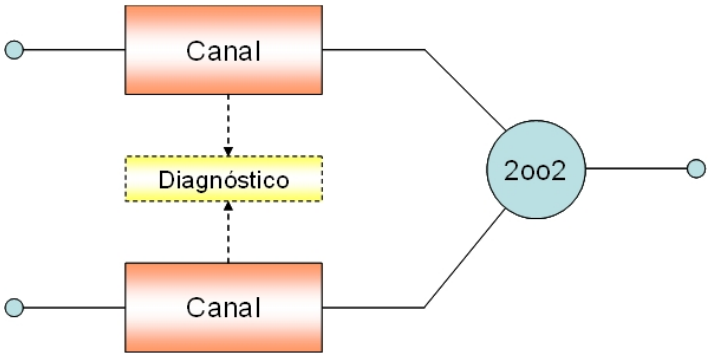


FIGURA 5.9: Diagrama de Bloco - Arranjo Físico (Arquitetura 2oo2)

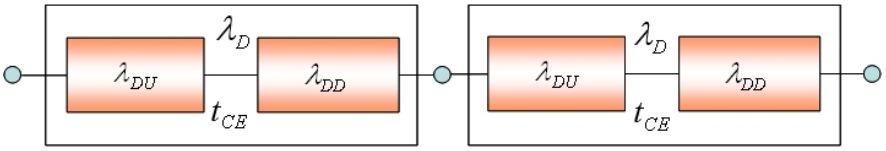


FIGURA 5.10: Diagrama de Blocos de Confiabilidade - Arquitetura 2oo2

Em um sistema 2oo2, os dois canais têm que funcionar para que o sistema funcione, ou seja, a falha de qualquer um deles é suficiente para causar a falha do sistema, portanto, como são dois canais sujeitos a falha, a taxa de falhas do sistema é duas vezes aquela de cada canal, ou seja:

$$\phi_{2oo2} = 2\phi_{1oo1} = 2\lambda_D \tag{5.43}$$

Por sua vez, o "tempo médio no estado falho" do sistema será o mesmo daquela calculado para cada canal (ver equação 5.8), pois a densidade de probabilidade será:

$$f_{2oo2} = 2 \cdot \lambda_{DU} e^{-2\lambda_{DU} t} \tag{5.44}$$

Como a densidade de probabilidade de falha aparece no numerador e no denominador (ver equação 5.7), o fator 2 desaparece e o resultado é $T_{2oo2} = T_1/2$ ou:

$$t_{CE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} \cdot MTTR \tag{5.45}$$

portanto:

$$PFD_{2oo2} = 2\lambda_D t_{CE} \tag{5.46}$$

que é a equação apresentada na Norma IEC 61508 (IEC-61508 1998) para esta arquitetura.

### 5.6.5 Arquitetura 2oo3

Esta arquitetura consiste de três canais conectados em paralelo com uma maioria votando arranjos para o sinal de saída, de tal forma que o estado de saída não é alterado se somente um canal apresentar um resultado diferente que discorde de outros dois canais. É assumido que qualquer teste de diagnóstico somente pode reportar as falhas encontradas e não pode mudar qualquer estado de saída ou alterar a votação de saída. As Figuras 5.11 e 5.12 ilustram os diagramas de bloco representativos desta arquitetura.

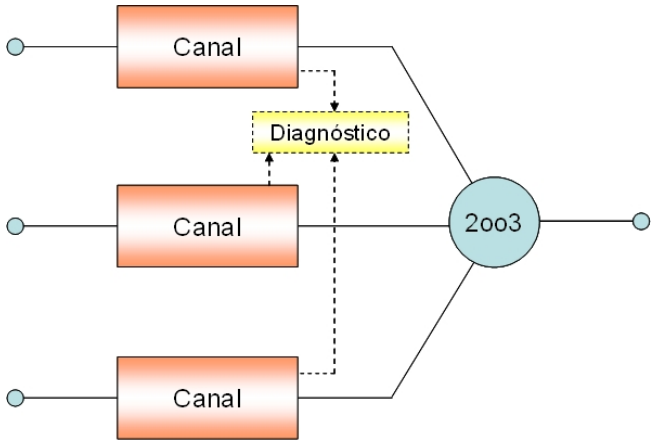


FIGURA 5.11: Diagrama de Bloco - Arranjo Físico - Arquitetura 2oo3

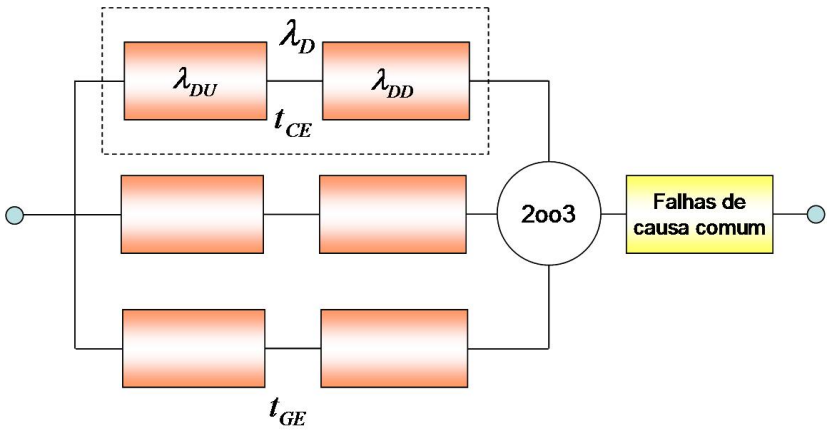


FIGURA 5.12: Diagrama de Blocos de Confiabilidade - Arquitetura 2oo3

Analogamente aos casos anteriores, tem-se:

$$PFD_{2oo3} = \phi_{2oo3} \cdot T_{2oo3} \tag{5.47}$$

Para a avaliação da freqüência $\phi_{2oo3}$, temos que levar em consideração a equação 5.25, que representa a taxa de falha equivalente de um sistema qualquer e a confiabilidade de um sistema com arquitetura 2oo3, conforme apresentado a seguir:

$$R_{2oo3} = 3R^2 - 2R^3 \qquad \text{ou ainda} \qquad R_{2003} = 3e^{-2\lambda t} - 2e^{-3\lambda t} \tag{5.48}$$

portanto, a densidade de probabilidade (ver equação 5.8) é:

$$f_{2oo3} = 6\lambda e^{-2\lambda t} - 6\lambda e^{-3\lambda t} \tag{5.49}$$

aproximando-se as exponenciais pelos três primeiros termos da série, chega-se a:

$$f_{2oo3} \cong 6\lambda_2 t \tag{5.50}$$

da mesma forma:

$$R_{2oo3} \cong 1 - 3\lambda_2 t_2 \tag{5.51}$$

e da equação 5.25, obtém-se:

$$\lambda_{2oo3}(t) = \frac{6\lambda_2 t}{1 - 3\lambda_2 t_2} \cong 6\lambda_2 t \tag{5.52}$$

Substituindo-se o resultado da equação 5.52 e fazendo as demais alterações necessárias para utilizar a equação 5.2, é possível calcular a freqüência média no intervalo [0,$T_1$] obtendo-se:

$$\phi_{2oo3} = \frac{1}{T_1} \int_0^{T_1} \lambda_{2oo3}(t)\, dt = 3\lambda_2 T_1 \tag{5.53}$$

e como $t_{CE} \cong T_1/2$, tem-se que:

$$\lambda_{2oo3}(t) = 6\lambda_2 t_{CE} \tag{5.54}$$

Para a avaliação de $T_{2oo3}$, ou seja, do valor médio do tempo que o sistema 2oo3 per-

manece no estado falho, pode-se calcular substituindo o valor encontrado para $f_{2oo3}(t)$ pela equação 5.50 na equação 5.7. Assim, é possível obter:

$$T_{2oo3} = \frac{\int_0^{T_1}(T_1 - t)6\lambda^2 t\, dt}{\int_0^{T_1} 6\lambda^2 t\, dt} = \frac{T_1}{3} \tag{5.55}$$

e incluindo as outras contribuições (dos reparos), obtém-se:

$$T_{2oo3} = t_{GE} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR)\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \tag{5.56}$$

Em função de tudo que foi descrito acima, é possível então calcular a PFD para um sistema com arquitetura 2oo3. Dado o apresentado na equação 5.47 e substituindo os resultados apresentados nas equações 5.53 e 5.55, tem-se:

$$PFD_{2oo3} = 6\lambda_D^2 t_{CE} t_{GE} \tag{5.57}$$

que é a equação apresentada na Norma IEC 61508 (IEC-61508 1998) para a PFD desta arquitetura.

## 5.7 Dedução da Fórmula de Cálculo da PFD para uma configuração *koon* qualquer

O Sistema *koon* é aquele que para funcionar necessita que pelo menos k dos seus n componentes funcionem. Portanto, é necessário que ocorra a falha de pelo menos (n-k+1) componentes para que o sistema falhe. Em outras palavras, de acordo com (MARSZAL & SCHARPF 2002), o primeiro "número", k, designa quantos elementos são requeridos para indicar a condição de *shutdown* e o segundo "número", n, designa quantos elementos no total são utilizados no sistema.

A PFD deste sistema pode ser escrita da seguinte forma:

$$PFD_{koon} = \phi_{koon} T_{koon} \tag{5.58}$$

### 5.7.1 Avaliação da Freqüência Média $\phi_{koon}$

A freqüência média de falhas no período [0,$T_1$] pode ser obtida como:

$$F(t) \cong \binom{n}{n-k+1}(\lambda t)^{n-k+1}(1-\lambda t)^{k-1} = \binom{n}{n-k+1}[(\lambda t)^{n-k+1} - (\lambda t)^n] \quad (5.59)$$

$$f(t) = \frac{dF(t)}{dt} = \binom{n}{n-k+1}\left[(n-k+1)\lambda^{n-k+1} \quad t^{n-k} - n\frac{(\lambda t)^n}{t}\right] \quad (5.60)$$

$$f(t) = \frac{dF(t)}{dt} = \binom{n}{n-k+1}\left[(n-k+1)\lambda^{n-k+1}t^{n-k}\right] \quad (5.61)$$

para $\lambda t >> 1 \rightarrow R(t) \rightarrow 1 \Rightarrow \lambda(t) \approx f(t)$ ou seja, $\lambda_{koon}(t) \approx f_{koon}(t)$

$$\phi_{koon} \cong \frac{1}{T_1}\binom{n}{n-k+1}(n-k+1)\frac{\lambda^{n-k+1}}{n-k+1}T_1^{n-k+1} \quad (5.62)$$

$$\phi_{koon} = n!\frac{\lambda^{n-k+1}}{(k-1)!(n-k+1)!}T_1^{n-k} \quad (5.63)$$

ou seja, a freqüência média pode ser expressa pela equação 5.63.

### 5.7.2 Avaliação do Tempo Médio no Estado Falho $T_{koon}$

Para a avaliação de $T_{koon}$, ou seja, do valor médio do tempo que o sistema *koon* permanece no estado falho, pode-se calcular substituindo o valor encontrado para $f_{koon}(t)$ pela equação 5.61, na equação 5.7. Assim, é possível obter:

$$T_{koon} = \frac{\binom{n}{n-k+1}(n-k+1)\lambda^{n-k+1}\int_0^{T_1}(T_1-t)t^{n-k}\,dt}{\binom{n}{n-k+1}(n-k+1)\lambda^{n-k+1}\int_0^{T_1}t^{n-k}dt}$$

$$T_{koon} = \frac{1}{\frac{T_1^{n-k+1}}{n-k+1}} \int_0^{T_1} (T_1 t^{n-k} - t^{n-k+1} dt = \frac{n-k+1}{T_1^{n-k+1}} \left[ \frac{T_1^{n-k+1}}{n-k+1} - \frac{T_1^{n-k+2}}{n-k+2} \right]$$

$$T_{koon} = \frac{n-k+1}{T_1^{n-k+1}} T_1^{n-k+2} \left[ \frac{1}{n-k+1} - \frac{1}{n-k+2} \right]$$

desta forma:

$$T_{koon} = \frac{T_1}{n-k+2} \tag{5.64}$$

$$T_{koon} = \frac{\lambda_{DU}}{\lambda_D} \left( \frac{T_1}{n-k+2} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \tag{5.65}$$

### 5.7.3 Avaliação $PFD_{koon}$

Em função de tudo que foi descrito acima, é possível então calcular a PFD para um sistema com arquitetura *koon*. Dado o apresentado na equação 5.58 e substituindo os resultados apresentados nas equações 5.63 e 5.65, temos:

$$PFD_{koon} = \underbrace{\frac{n!}{(k-1)!(n-k+1)!} \lambda^{n-k+1} T_1^{n-k}}_{\phi_{koon}} \underbrace{\frac{T_1}{n-k+2}}_{T_{koon}}$$

ou seja:

$$PFD_{koon} = \frac{n!}{(k-1)!(n-k+2)!} \lambda^{n-k+1} T_1^{n-k+1} \tag{5.66}$$

### 5.7.4 Avaliação de $PFD_{koon}$ considerando a contribuição do reparo

A equação 5.66 fornece a $PFD_{koon}$ sem considerar a contribuição do reparo para a indisponibilidade do sistema (somente a contribuição das falhas não detectadas durante o intervalo entre testes). Para incluir a contribuição do reparo, deve-se tomar o

"tempo médio no estado falho" para o sistema *koon* dado pela equação 5.65, ou seja, multiplicando esta equação pela equação 5.63, chega-se a:

$$PFD_{koon} = \frac{n!}{(k-1)!(n-k+1)!}(\lambda_D^{n-k+1} T_1^{n-k}) \times \left[\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{n-k+2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR\right] \quad (5.67)$$

De forma a validar as equações 5.63, 5.65, 5.66 e 5.67 proposta para sistemas *koon*, o Apêndice A deste trabalho apresenta a aplicação das mesmas nas arquiteturas apresentadas nas seções anteriores pelo IEC e também em algumas outras de uso mais comum na indústria.

## 5.8 Modelagem das Falhas de Causa Comum

Sistemas de segurança normalmente utilizam redundâncias que são incorporadas para prover uma alta probabilidade de sucesso dos mesmos. Quando quantificada a probabilidade de sucesso, os sub-sistemas redundantes não irão sempre falhar independentemente. Uma causa de falha comum pode afetar canais redundantes num mesmo momento. Em estudos de segurança os cálculos devem levar em conta estas falhas de causa comum (FCC).

De acordo com a Parte 4 da Norma IEC 61508 (IEC-61508-4 1998), falhas de modo comum são falhas que são o resultado de um ou mais eventos, causando falhas de dois ou mais canais separados em sistemas com canais mútiplos, levando à falha do sistema.

Conforme discutido na seção 2.3.2.2, diversos modelos paramétricos têm sido propostos na literatura para a modelagem de falhas de causa comum, como por exemplo o modelo de Múltiplas Letras Gregas, modelo do Fator Alpha, e o modelo do Fator Beta. O modelo do Fator Beta talvez seja atualmente um dos mais utilizados para falhas de causa comum, e é o que a Norma referência deste trabalho, IEC 61508 (IEC-61508 1998), adota.

O Método do Fator Beta assume que os efeitos de causa comum podem ser repre-

sentados no modelo de confiabilidade do sistema como uma proporção da probabilidade de falha de qualquer canal único de canais múltiplos de sistemas redundantes. Onde os canais têm diferentes níveis de complexidade, o fator beta é aplicado a taxa de falha estimada ou à probabilidade do canal de maior confiabilidade (ANDREWS & MOSS 2002).

### 5.8.1 O Modelo do Fator Beta ($\beta$)

Considere-se um sistema composto de $n$ componentes idênticos, cada um com taxa de falha constante $\lambda$. A falha de um determinado componente pode ocorrer devido a duas causas possíveis:

- Fatores relacionados somente ao componente em questão e portanto independentes da condição dos outros componentes do sistema;

- Ocorrência de um evento externo, porém independente do sistema, mas que acarreta a falha simultânea de todos os componentes do sistema.

Seja $\lambda_i$ a taxa de falha devido à primeira causa (independente), e seja $\lambda_c$ a taxa de falha devido ao segundo tipo de causa (dependente - causa comum). Assumindo independência entre os dois tipos de causas de falha, a taxa de falha total $\lambda$ de cada componente é simplesmente a soma das taxas de falha dos dois tipos de causas:

$$\lambda = \lambda_i + \lambda_c \tag{5.68}$$

O fator $\beta$ é definido como a fração da taxa de falha comum sobre a taxa de falha total, ou seja, representa a proporção relativa de falhas de causa comum dentro de todas as falhas de um componente:

$$\beta = \frac{\lambda_c}{\lambda} \qquad \text{ou} \qquad \lambda cc = \beta \cdot \lambda \tag{5.69}$$

e

$$\lambda_i = \lambda - \lambda_c = (1 - \beta) \cdot \lambda \tag{5.70}$$

Cabe destacar que neste modelo, a probabilidade de ocorrerem falhas simultâneas de um número parcial de componentes é nula.

Conforme apresentado na Tabela 5.1, a Norma do IEC 61508 também considera o parâmetro $\lambda_D$, que representa o percentual da taxa de falha total do componente que pode ser considerada como falha de causa comum detectada.

O Anexo D da Parte 6 da Norma IEC 61508 (IEC-61508-6 2000) apresenta uma metodologia para o cálculo de $\beta$ e $\beta_D$, sendo que esta metodologia é limitada a falhas de causa comum de *hardware* e baseada em julgamentos de engenharia e não abrange as falhas de causa comum causadas por *software* ou pela complexidade do processo.

### 5.8.2 Modelagem das Falhas de Causa Comum nas Fórmulas de Cálculo de PFD da Norma IEC 61508

A seção 5.6 apresentou as deduções das fórmulas de cálculo da probabilidade de falha na demanda para diversas configurações, de acordo com o proposto pela metodologia da Norma IEC 61508, considerando inclusive a contribuição do reparo para estes cálculos. Esta seção tem o objetivo de apresentar as referidas fórmulas, levando em consideração também a probabilidade de ocorrerem falhas de causa comum que afetem os componentes das alternativas consideradas.

#### 5.8.2.1 Arquitetura 1oo2

Considerando o discutido na seção 5.6.2 e a equação 5.39, é possível expandir esta equação de forma a considerar as falhas de causa comum:

$$PFD_{1oo2} = 2\left[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right]^2 t_{CE} t_{GE} + \\ + \beta_D \lambda_{DD} MTTR + \beta \lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) \tag{5.71}$$

que é a equação apresentada na Norma IEC 61508 (IEC-61508-6 2000) para esta arquitetura.

#### 5.8.2.2 Arquitetura 1oo2D

Considerando o discutido na seção 5.6.3 e as equações 5.40, 5.41 e 5.42, é possível expandir esta equação de forma a considerar também as falhas de modo comum:

$$PFD_{1oo2D} = 2(1-\beta)\lambda_{DU}\left[(1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD} + \lambda_{SD}\right] t'_{CE} t'_{GE} + \\ + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) \quad (5.72)$$

que é a equação apresentada na Norma IEC 61508 (IEC-61508-6 2000) para esta arquitetura.

#### 5.8.2.3 Arquitetura 2oo3

Considerando o discutido na seção 5.6.5 e a equação 5.57, é possível expandir esta equação de forma a considerar as falhas de causa comum:

$$PFD_{2oo3} = 6\left[(1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD}\right]^2 t_{CE} t_{GE} + \\ + \beta_D \lambda_{DD} MTTR + \beta\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) \quad (5.73)$$

que é a equação apresentada na Norma IEC 61508 (IEC-61508-6 2000) para esta arquitetura.

### 5.8.3 Modelagem das Falhas de Causa Comum nas Fórmulas de Cálculo de PFD de uma Arquitetura koon

Considerando o discutido na seção 5.7.4 e a equação 5.67, é possível expandir esta equação de forma a considerar também as falhas de causa comum para arquiteturas *koon* quaisquer:

$$PFD_{koon} = \left[\frac{n!}{(k-1)!(n-k+1)!}\left[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right]^{n-k+1} T_1^{n-k}\right] \times$$

$$\left[\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{n-k+2}+MTTR\right)+\frac{\lambda_{DD}}{\lambda_D}MTTR\right]+\beta_D\lambda_{DD}MTTR$$
$$+\beta\lambda_{DU}\left(\frac{T_1}{2}+MTTR\right) \quad (5.74)$$

## 5.9 O Fator Diagnóstico de Cobertura (DC)

A confiabilidade e a segurança de sistemas automáticos de controle dependem de um grande número de fatores. Um dos mais importantes, tanto em arquiteturas redundantes quanto em não redundantes, é a habilidade do sistema em detectar falhas dos componentes: diagnósticos *on-line*. A maior parte dos equipamentos eletrônicos, realiza periodicamente testes internos, ou seja, a cada sinal enviado realiza um auto diagnóstico e verifica se o seu sistema está ou não falho. Conforme destacado acima, a habilidade de detectar uma falha é uma importante característica em qualquer sistema de controle ou de segurança. Esta característica pode ser usada para reduzir o tempo de reparo e para controlar a operação de várias arquiteturas tolerantes a falhas. A medida desta habilidade é conhecida como fator de cobertura de diagnóstico. O fator de cobertura de diagnóstico mede a probabilidade de que uma falha seja detectada, dado que ela ocorra (GOBLE 1998). Este diagnóstico de cobertura, um número entre 0 e 1, é calculado adicionando as taxas de falha de falhas detectadas e dividindo a mesma pela taxa de falha total do sistema.

A capacidade de diagnóstico é limitada pelo componente/dispositivo selecionado e por diagnósticos externos que podem ser utilizados com o mesmo. Por exemplo, se entradas discretas, como sensores são utilizados, muito pouca cobertura de diagnóstico estará disponível, mesmo quando se utiliza redundância. Quando se usam componentes/dispositivos analógicos são utilizados, os sinais de componentes/ dispositivos redundantes podem ser comparados. Quando os sinais diferem de forma inaceitável, um alarme pode ser gerado, alertando o operador que o reparo deve ser iniciado. Isto fornece o diagnóstico de cobertura (FRANCISCO 1993).

A definição formal da Norma IEC 61508 para este fator de diagnóstico de cobertura é uma fração de diminuição da probabilidade de falhas perigosas de *hardware* resultante da operação de testes de diagnóstico automáticos (IEC-61508-4 1998). O DC pode também ser expresso em termos da equação 5.75, onde $\lambda_{DD}$ é a probabilidade de falhas

perigosas detectadas e $\lambda_{Dtotal}$ é a probabilidade total de falhas.

$$DC = \frac{\sum \lambda_{DD}}{\sum \lambda_{Dtotal}} \tag{5.75}$$

É importante destacar que o diagnóstico de cobertura pode existir para todas as partes do SIS. Por exemplo, pode existir somente para sensores e/ou sistemas de lógica e/ou elementos finais.

Um método para calcular o fator de diagnóstico de cobertura é apresentada no Anexo C da parte 2 da Norma do IEC 61508 (IEC-61508-2 2000). Estes dados também podem ser encontrados em banco de dados como o SINTEF (HAUGE, HOKSTAD, LANGSETH & OIEN 2006).

## 5.10 Testes Imperfeitos

Conforme discutido anteriormente, existem diversos tipos de falha. Um estado de falha é aquele em que o equipamento não desempenha mais sua função de acordo com os padrões mínimos aceitáveis. A falha não se refere ao equipamento como um todo, mas sim às funções que ele se propõe a desempenhar. A falha pode ser considerada evidente, quando sua manifestação se torna aparente para as pessoas, ou pode ser considerada oculta, quando sua manifestação não se torna aparente. A falha oculta é bastante comum em instalações redundantes, sistemas de segurança e de alarme, que normalmente estão inoperantes. Então elas só se tornam evidentes quando demandadas e não respondem.

Falhas no sistema de segurança que não são detectadas nem pelo diagnóstico de cobertura e nem pelos testes periódicos, são identificadas/percebidas somente no momento de uma demanda que requeira a função de segurança afetada por esta falha. Desta forma, para estas falhas totalmente não detectadas, a taxa de demanda esperada do sistema de segurança governa o tempo efetivo de parada do sistema. Dado esta descrição é possível destacar que para a Norma IEC 61508, os chamados "testes imperfeitos" são os testes do sistema de segurança que possuem falhas que não conseguem ser detectadas a não ser no momento de uma demanda real.

Para considerar esta possibilidade para o cálculo da PFD de sistemas de segurança,

de acordo com a IEC 61508, é necessário fazer algumas adaptações nas fórmulas apresentadas anteriormente neste capítulo (seção 5.6), como por exemplo, assumir dois novos parâmetros: o tempo entre demandas (em horas) e um coeficiente que representa a fração das falhas DU (falhas perigosas e não detectadas) que somente são identificadas durante a demanda do sistema. Assumimos aqui serem estes parâmetros, $T_2$ e $C$, respectivamente. Cabe ressaltar que $T_1$ representa o intervalo entre testes totais do sistema.

Desta forma, esta seção tem como objetivo, além de discutir os conceitos de testes imperfeitos de sistemas de segurança, apresentar as fórmulas para o cálculo da probabilidade de falha na demanda, considerando a possibilidade de levar em consideração que os testes do sistema de segurança podem ser "imperfeitos" e não eliminar todas as possíveis falhas que o sistema poderia vir a sofrer, ou seja, mesmo testando o sistema de segurança, ele não volta a poder ser considerado "tão bom quanto novo".

Cabe ressaltar que a IEC 61508 apresenta apenas a expressão para cálculo da PFD considerando testes imperfeitos, para uma arquitetura 1oo2. As demais arquiteturas aqui apresentadas foram desenvolvidas em analogia a este resultado.

### 5.10.1 Arquitetura 1oo1

Considerando testes imperfeitos de sistemas de segurança e o discutido na seção 5.6.1, é possível verificar que o "tempo médio no estado falho equivalente" para o canal, ou $t_{CE}$, é igual a:

$$t_{CE} = \frac{(1-C)\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{C\lambda_{DU}}{\lambda_D}\left(\frac{T_2}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR \quad (5.76)$$

e a PFD, conseqüentemente, em função da equação 5.20, pode ser reescrita como:

$$PFD_{1oo1} = \lambda_D \times \left[\frac{(1-C)\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{C\lambda_{DU}}{\lambda_D}\left(\frac{T_2}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR\right] \quad (5.77)$$

### 5.10.2 Arquitetura 1oo2

Considerando testes imperfeitos de sistemas de segurança e o discutido na seção 5.6.2, é possível verificar que o valor médio do tempo que um canal do sistema 1oo2 permanece no estado falho, ou $t_{CE}$, e o tempo médio no estado falho para esta configuração $t_{GE}$, valem respectivamente:

$$t_{CE} = \frac{(1-C)\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{C\lambda_{DU}}{\lambda_D}\left(\frac{T_2}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR \quad (5.78)$$

$$t_{GE} = \frac{(1-C)\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{C\lambda_{DU}}{\lambda_D}\left(\frac{T_2}{3} + MTTR)\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR \quad (5.79)$$

e a PFD, conseqüentemente, em função das equações 5.39 e 5.71, pode ser reescrita como:

$$\begin{aligned} PFD_{1oo2} = {} & 2\left[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right]^2 t_{CE}t_{GE} + \beta_D\lambda_{DD}MTTR \\ & + \beta(1-C)\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) + \beta C\lambda_{DU}\left(\frac{T_2}{2} + MTTR\right) \end{aligned} \quad (5.80)$$

### 5.10.3 Arquitetura 1oo2D

Considerando testes imperfeitos de sistemas de segurança e o discutido na seção 5.6.3, é possível verificar que ao valor médio do tempo que um canal do sistema 1oo2D permanece no estado falho, ou $t_{CE}^{'}$, e o tempo médio no estado falho para esta configuração $t_{GE}^{'}$, valem respectivamente:

$$\begin{aligned} t_{CE}^{'} = {} & \frac{(1-C)\lambda_{DU}}{\lambda_{DU}+\lambda_{DD}+\lambda_{SD}}\left(\frac{T_1}{2} + MTTR\right) + \frac{C\lambda_{DU}}{\lambda_{DU}+\lambda_{DD}+\lambda_{SD}}\left(\frac{T_2}{2} + MTTR\right) \\ & + \frac{\lambda_{DD}}{\lambda_{DU}+\lambda_{DD}+\lambda_{SD}}MTTR \end{aligned} \quad (5.81)$$

$$t_{GE}^{'} = \frac{(1-C)\lambda_{DU}}{\lambda_{DU}+\lambda_{DD}+\lambda_{SD}}\left(\frac{T_1}{3}+MTTR\right) + \frac{C\lambda_{DU}}{\lambda_{DU}+\lambda_{DD}+\lambda_{SD}}\left(\frac{T_2}{3}+MTTR\right) + \frac{\lambda_{DD}+\lambda_{SD}}{\lambda_{DU}+\lambda_{DD}+\lambda_{SD}}MTTR \quad (5.82)$$

e a PFD, conseqüentemente, em função das equações 5.40 e 5.72, pode ser reescrita como:

$$PFD_{1oo2D} = 2(1-\beta)\lambda_{DU}\left[(1-\beta)\lambda_{DU}+(1-\beta_D)\lambda_{DD}+\lambda_{SD}\right]t_{CE}^{'}t_{GE}^{'} + \\ + \beta_D\lambda_{DD}MTTR + \beta(1-C)\lambda_{DU}\left(\frac{T_1}{2}+MTTR\right) + \beta C\lambda_{DU}\left(\frac{T_2}{2}+MTTR\right) \quad (5.83)$$

### 5.10.4 Arquitetura 2oo2

Considerando testes imperfeitos de sistemas de segurança e o discutido na seção 5.6.4, é possível verificar que o "tempo médio no estado falho equivalente" para o canal, ou $t_{CE}$, é igual a:

$$t_{CE} = \frac{(1-C)\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2}+MTTR\right) + \frac{C\lambda_{DU}}{\lambda_D}\left(\frac{T_2}{2}+MTTR\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR \quad (5.84)$$

e a PFD, conseqüentemente, em função da equação 5.46, pode ser reescrita como:

$$PFD_{2oo2} = 2\lambda_D \times \\ \left[\frac{(1-C)\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2}+MTTR\right) + \frac{C\lambda_{DU}}{\lambda_D}\left(\frac{T_2}{2}+MTTR\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR\right] \quad (5.85)$$

### 5.10.5 Arquitetura 2oo3

Considerando testes imperfeitos de sistemas de segurança e o discutido na seção 5.6.5, é possível verificar que o valor médio do tempo que um canal do sistema 2oo3 permanece no estado falho, ou $t_{CE}$, e o tempo médio no estado falho para esta configuração $t_{GE}$ são iguais respectivamente a:

$$t_{CE} = \frac{(1-C)\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{C\lambda_{DU}}{\lambda_D}\left(\frac{T_2}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR \quad (5.86)$$

$$t_{GE} = \frac{(1-C)\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{C\lambda_{DU}}{\lambda_D}\left(\frac{T_2}{3} + MTTR)\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR \quad (5.87)$$

e conseqüentemente a PFD, em função das equações 5.57 e 5.73, pode ser reescrita como:

$$PFD_{2oo3} = 6\left[(1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD}\right]^2 t_{CE}t_{GE} + \\ + \beta_D\lambda_{DD}MTTR + \beta(1-C)\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) + \beta C\lambda_{DU}\left(\frac{T_2}{2} + MTTR\right) \quad (5.88)$$

### 5.10.6 Arquitetura 1oo2 segundo IEC 61508

Cabe ressaltar que a parte 6 da Norma IEC 61508 (IEC-61508-6 2000) apresenta como exemplo a equação de cálculo para um sistema 1oo2 e considera que 50% das falhas DU (falhas perigosas e não detectadas) são detectadas somente durante a demanda do sistema, ou seja, mesmo que se teste o sistema regularmente, algumas falhas somente serão reveladas no momento de uma demanda do sistema, o que implica em dizer que os testes do sistema são imperfeitos. Considerando $T_2$ como o tempo entre demandas para uma configuração 1oo2, os termos $t_{CE}$ e $t_{GE}$ podem ser expressos por:

$$t_{CE} = \frac{\lambda_{DU}}{2\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DU}}{2\lambda_D}\left(\frac{T_2}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR \quad (5.89)$$

e

$$t_{GE} = \frac{\lambda_{DU}}{2\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DU}}{2\lambda_D}\left(\frac{T_2}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR \quad (5.90)$$

e a PFD conseqüentemente:

$$PFD_{1oo2} = 2\left[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right]^2 t_{CE}t_{GE} + \beta_D\lambda_{DD}MTTR + \\ + \beta\frac{\lambda_{DU}}{2}\left(\frac{T_1}{2} + MTTR\right) + \beta\frac{\lambda_{DU}}{2}\left(\frac{T_2}{2} + MTTR\right) \quad (5.91)$$

## 5.11 Testes Parciais dos Sistemas de Segurança

Dadas as características dos equipamentos de segurança, todo o equipamento de proteção deve ser regularmente testado ou pode não atuar quando necessário. O teste deve ser o mais completo possível e simular condições reais. No entanto, testes parciais podem ser utilizados para complementar os testes totais do sistema com o intuito de reduzir a probabilidade de falha na demanda do mesmo sem a necessidade da parada da planta para a sua realização.

Existem diversos métodos para a realização de testes parciais disponíveis para o usuário. Cada método apresenta diferentes componentes para facilitar o teste e deve ser avaliado individualmente para verificação do seu específico impacto para o SIL do sistema de segurança. Outro ponto a destacar é que, dado que os testes são realizados automaticamente pelo sistema, custos com mão-de-obra são minimizados, permitindo em muitos casos, atingir o SIL requerido sem causar impactos nos custos de manutenção e operação (SUMMERS & ZACHARY 2002).

É visível pelos dados disponíveis na literatura, por exemplo, no OREDA ((OREDA 2002)), que a maior proporção de falhas não detectadas é relacionada aos elementos finais, por exemplo, uma válvula de *shutdown*. Um teste parcial desta válvula pode ser definido, por exemplo, como permitir ao sistema de segurança fechar a válvula somente 20%. Neste caso, todos os elementos estariam sendo testados, entretanto a válvula nunca fecha completamente durante o teste.

Para considerar a possibilidade de realização de testes parciais de componentes do sistema de segurança nos cálculos da PFD dos mesmos, é necessário fazer algumas adaptações nas equações apresentas anteriormente neste capítulo (seção 5.6). É necessário assumir dois novos parâmetros: o intervalo de tempo entre testes parciais do sistema/componente e um coeficiente que represente a fração das falhas DU (falhas perigosas e não detectadas) que conseguem ser detectadas durante testes parciais do

sistema. Assumimos aqui serem estes parâmetros, $T_2$ e $C$, respectivamente.

Desta forma, é possível verificar que as expressões apresentadas na seção 5.10, para as arquiteturas 1oo1, 1oo2, 1oo2D, 2oo2 e 2oo3 são válidas para cálculos de PFD considerando testes parciais de elementos do sistema em análise, sendo que para esta utilização, o parâmetro $T_2$ deve ser entendido como o intervalo entre testes parciais do sistema (em horas) e o parâmetro $C$, um coeficiente que representa a fração das falhas DU (falhas perigosas e não detectadas) que são identificadas durante testes parciais do sistema.

Cabe destacar que a Norma IEC 61508 não apresenta as equações para cálculo da PFD considerando a possibilidade de realização de testes parciais. A proposição aqui apresentada foi desenvolvida em analogia ao sugerido pela mesma para a consideração de testes imperfeitos.

# Capítulo 6

# Estudo de Caso: Análise de um Sistema de Bloqueio para Proteção do Header de Flare

## 6.1 Introdução

Uma das questões mais importantes para a segurança de plantas de processos é a prevenção de eventos de perda de contenção causados por pressão excessivamente alta. Um acidente com perda de contenção por alta pressão pode ter graves conseqüências para os trabalhadores, o meio ambiente e para o patrimônio da empresa, devido à possibilidade de ocorrência de uma grande liberação de produtos tóxicos ou inflamáveis. Para se evitar esse tipo de problema, é fato conhecido dos projetistas dessas plantas que todos os vasos de pressão (aqui incluídos todos os equipamentos que, de alguma forma, acumulam líquidos ou gases pressurizados, tais como colunas, torres, separadores, etc.), devem ser dotados de sistemas de alívio para proteção dos mesmos contra eventuais episódios de alta pressão.

As normas de projeto mais utilizadas pelo setor, tais como as do API-RP 521 (ANSI/API-521 1997) e do ASME (ASME-BPCV-VIII 2004) fornecem critérios para a proteção de vasos contra pressurização excessiva. Tradicionalmente, essa proteção têm sido feita com a colocação de dispositivos de alívio, tais como válvulas de alívio ou discos de ruptura. No Brasil, a Norma Regulamentadora NR-13 (NR-13 1994) também

exige a colocação de tais dispositivos de alívio.

Nos Estados Unidos, a partir de 1996, com a aprovação do "Code Case 2211 of ASME Section VIII" (ASME 1996), e da $4^a$ edição da Prática Recomendada RP-521, foram estabelecidas algumas condições para as quais seria admitida a utilização de sistemas instrumentados de segurança (SIS) como meio de proteção contra alta pressão em vasos de processos. Como garantia, as normas exigem que em caso de utilização de um SIS, este forneça um grau de segurança maior ou pelo menos igual ao fornecido pelos dispositivos de alívio. De um modo geral, para que isso seja conseguido, o SIS deve ter uma probabilidade de falha muito baixa, o que invariavelmente acarreta que seja projetado para atender a SIL 3. Em função do alto nível de confiabilidade exigido, tais sistemas ficaram conhecidos como HIPPS, do inglês "High Integrity Pressure Protection Systems". A Norma do ASME especifica bem os casos em que um HIPPS pode ser usado em lugar dos dispositivos de alívio, mas o API RP-521 recomenda que um HIPPS seja usado somente nos casos em que os dispositivos de alívio sejam "impraticáveis", sem, no entanto, esclarecer o que esse termo efetivamente representa.

Um dos casos onde o HIPPS vem sendo cada vez mais utilizado é em ampliações de instalações petroquímicas existentes: novas unidades são instaladas fazendo com que o *header* do flare existente não tenha mais capacidade para resistir ao aumento de pressão causado pela despressurização simultânea de todas as unidades da instalação. Tais eventos de despressurização conjunta podem ocorrer em casos de perdas de elementos comuns a todas, tais como energia elétrica ou outras utilidades. A solução seria a substituição do flare existente por um novo de maior capacidade, o que poderia representar um grande investimento para a empresa. Uma alternativa que pode ser economicamente atrativa é a da colocação de sistemas do tipo HIPPS para prover o bloqueio da fonte de energia para uma ou mais das novas unidades, o que evita a despressurização destas novas unidades em conjunto com as unidades existentes. Deste modo, o *header* existente poderia permanecer com a sua capacidade atual, pois permaneceria recebendo apenas a descarga das unidades existentes. Na prática, as novas unidades seriam também dotadas de válvula de alívio, o que, no caso brasileiro, continuaria atendendo à NR-13, mas o sistema HIPPS seria, efetivamente, o sistema de proteção contra pressão alta no vaso. Em um evento de despressurização conjunta, a falha do HIPPS de uma planta nova causaria a ruptura do *header* do flare devido

à pressão excessiva no mesmo. Em caso de um desvio de alta pressão localizado somente na nova instalação, a falha do HIPPS não teria maiores conseqüências, pois neste caso haveria a possibilidade de abertura da válvula de alívio e a conseqüente despressurização da unidade para o flare.

Como mencionado anteriormente, tipicamente no caso da proteção do *header* do flare seria exigido que o HIPPS atendesse a um SIL Requerido igual a 3, o que não necessariamente teria que ser o caso (dependendo dos resultados da análise de riscos para a determinação do SIL requerido, conforme discutido nos capítulos 2, 3 e 4). Restaria então, verificar qual a melhor estratégia para se atender a este alto nível de SIL, ou seja, como conseguir atender a esta exigência da forma mais eficiente possível. A solução deste problema passa necessariamente pela realização de uma análise custo-benefício das várias alternativas de configuração do SIS e das suas políticas de teste, conforme também já mencionado em capítulos anteriores deste trabalho. No presente capítulo, é apresentado um estudo de caso envolvendo a solução de um problema de escolha entre alternativas para a configuração de um SIS para bloqueio da fonte de energia para uma coluna de separação, de modo a evitar que a mesma despressurize para o *header* do flare em caso de parada conjunta de todas as unidades de uma grande planta petroquímica.

O problema objeto do presente estudo de caso é apresentado na Seção 6.2, a descrição do sistema analisado é feita na Seção 6.3 e as alternativas analisadas são detalhadas na Seção 6.5. As premissas da análise e os dados utilizados nos cálculos são apresentados na Seção 6.6 e os resultados obtidos são mostrados e discutidos na Seção 6.7. Finalmente, a análise de sensibilidade do resultado obtido e os comentários finais sobre o estudo de caso são apresentados na Seção 6.8.

## 6.2 Apresentação do Problema Analisado

Na realização de um projeto de expansão de uma grande planta petroquímica, à qual seriam adicionadas duas novas unidades de processo, foi verificado que o *header* do flare não teria capacidade para receber a descarga resultante da despressurização conjunta das unidades novas e existentes em caso de um desligamento súbito de todas as unidades da instalação. Neste caso, a solução tradicional obrigaria à ampliação do *header* atual

ou à construção de um novo *header* para atender à demanda das unidades novas. Ambas as soluções envolvem altos custos e causariam sérios transtornos operacionais.

Em linha com as novas possibilidades abertas pelas atuais normas de projeto (conforme indicado na Seção 6.1), os responsáveis pelo projeto buscaram a solução do problema através da utilização de um Sistema HIPPS. Neste caso, a função do HIPPS seria a de bloquear a fonte de energia (vapor) para o refervedor da torre principal de uma das novas unidades no momento de um desligamento súbito conjunto de todas as unidades da instalação.

Uma análise de risco foi conduzida para a determinação do SIL requerido para o novo Sistema de Bloqueio do Refervedor (Sistema HIPPS), a qual investigou todos os cenários de acidente que levariam à despressurização da torre para o flare e concluiu pela necessidade de atendimento à SIL 3, ou seja, a sua PFD deve estar entre $1,0 \times 10^{-4}$ e $1,0 \times 10^{-3}$, para a proteção do *header* no caso dos eventos de despressurização conjunta de todas as unidades (tais como perda de energia elétrica ou falhas de outras utilidades comuns). Esta análise de risco para a determinação do SIL requerido não faz parte do escopo do presente trabalho.

O problema analisado neste capítulo consiste exatamente na realização de uma detalhada análise custo-benefício para a escolha da alternativa mais eficiente para a configuração do Sistema de Bloqueio do Refervedor, de modo que o mesmo atenda ao requisito de SIL 3. Conforme discutido anteriormente, em uma análise custo-benefício, a alternativa mais eficiente é a que apresenta a melhor relação custo-benefício, considerando-se os custos incorridos e os benefícios auferidos ao longo de todo o ciclo de vida do sistema.

## 6.3 Descrição do Sistema Analisado

Um diagrama esquemático representativo de toda a instalação petroquímica está apresentado na Figura 6.1, na qual podem ser vistos, o *header* do flare para o qual descarregam tanto as unidades existentes quanto as novas, a torre da nova unidade a ser protegida e o seu refervedor, onde será instalado o sistema de bloqueio. Na Figura 6.2, são apresentados mais detalhes do sistema de bloqueio analisado neste trabalho.

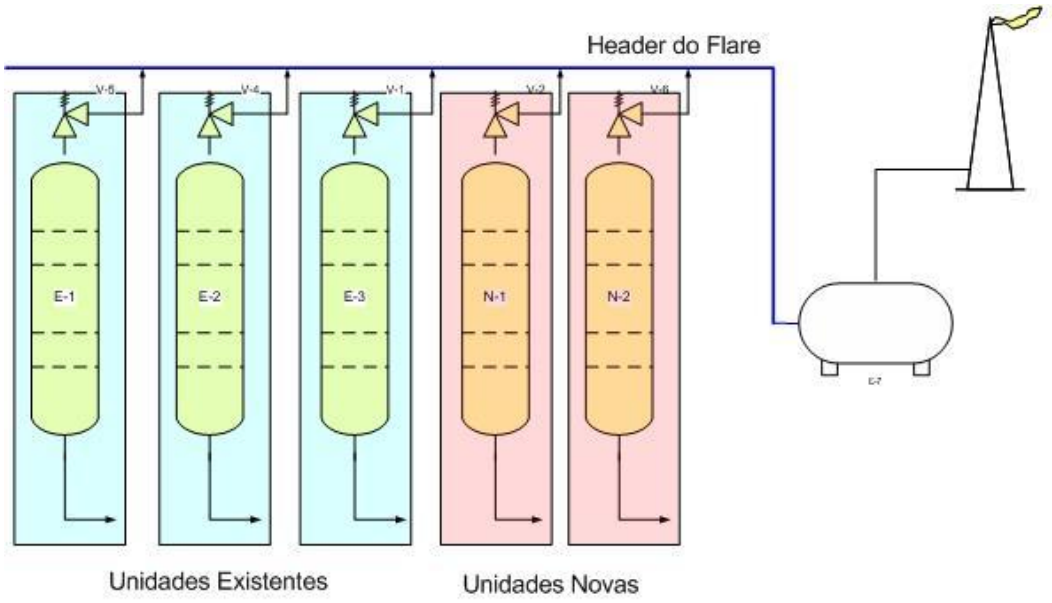


FIGURA 6.1: Instalação Considerada

O Sistema de Bloqueio do Refervedor, doravante denominado SBR, é um sistema instrumentado de segurança (SIS) e como tal, é formado por três partes básicas: iniciador, unidade lógica e atuador. Na sua alternativa mais básica, o iniciador seria um único pressostato (ou transmissor de pressão), a unidade lógica seria um CLP (do tipo simplex) e o atuador seria uma única válvula de bloqueio (com a sua válvula solenóide associada). Esta é a configuração mostrada na Figura 6.2. Um grande número de outras configurações são possíveis e várias delas são analisadas na próxima seção deste capítulo.

A função de segurança do SBR consiste em bloquear rapidamente a entrada de vapor (fonte de energia) para o refervedor R-01 da torre T-01, impedindo a sua pressurização e conseqüente despressurização para o *flare* através da válvula de alívio, em caso de um desligamento súbito conjunto de todas as unidades da instalação. A falha no cumprimento desta função acarretaria uma pressurização excessiva do *header* do *flare*, levando à sua ruptura e, conseqüentemente à liberação de grande quantidade de gases inflamáveis para a atmosfera no perímetro da instalação.

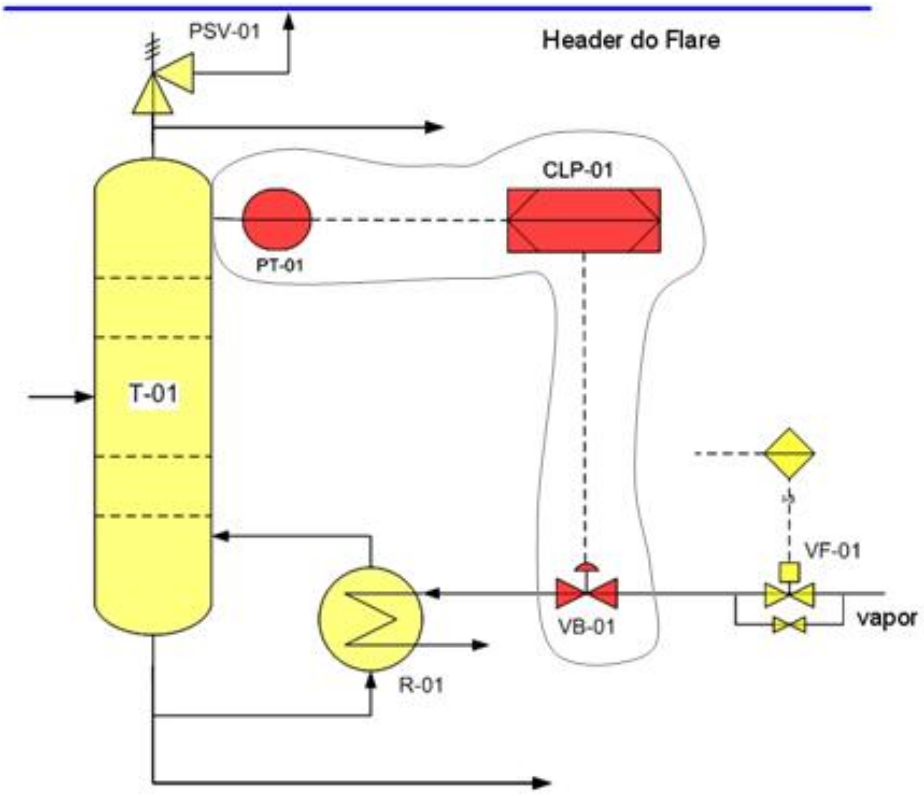


FIGURA 6.2: Sistema de Bloqueio

Conforme indicado na Figura 6.2, além da válvula de bloqueio VB-01, na linha de vapor para o refervedor existe também uma válvula de controle de fluxo VF-01 para controlar a admissão de vapor para o R-01 em função da temperatura da torre T-01. Buscando-se a separação total entre o sistema de controle e o sistema de segurança, esta válvula não foi considerada como parte do SBR em nenhuma das configurações analisadas. No entanto, embora a separação controle-segurança seja recomendada, a Norma IEC 61508 não veda a possibilidade de se dar crédito a válvulas de controle para a execução de funções de segurança, sob determinadas condições. A principal preocupação da norma refere-se à necessidade de independência do elemento de controle em relação aos eventos responsáveis pela demanda da atuação do sistema de segurança. Conforme explicado a seguir, no presente caso, a falha do elemento de controle não poderia ser responsável pela demanda da função de segurança do SBR. Como uma abertura descontrolada da VF-01 (um modo de falha da válvula de controle) levaria a um aumento de pressão na torre, poderia parecer em princípio que esta relação excluiria a possibilidade da VF-01 ser considerada como parte do SBR. No entanto, esta falha levaria à necessidade de despressurização unicamente da T-01 e não a uma

despressurização conjunta de todas as unidades da instalação. Para esse problema, o sistema de segurança é a válvula de alívio e não o SBR. Obviamente que o SBR também atuaria através do fechamento da VB-01, mas esta não é a função para o qual está sendo projetado, pois o mesmo está sendo colocado para atuar em caso de uma despressurização conjunta de todas as unidades e não daquela relativa unicamente à torre T-01. Por sua vez, dar crédito à VF-01 como elemento do SBR exigiria um cuidado especial com vários outros fatores, que não são objeto do presente trabalho.

## 6.4 Estratégias para Atendimento ao SIL Requerido

Conforme citado anteriormente, uma importante medida de capacidade de redução de risco de uma Função Instrumentada de Segurança, FIS, é o atributo de confiabilidade PFD, ou Probabilidade de Falha na Demanda. A FIS deve ser projetada e configurada para atingir o SIL requerido pelo processo. Assim, a PFD para a FIS deve estar na faixa de PFD especificada para o SIL exigido, conforme valores apresentados na Tabela 3.1. Se não estiver, será necessário reprojetar a FIS ou buscar outra alternativa que garanta o atendimento a este requisito.

Dado este cenário, é possível apresentar e discutir brevemente possíveis estratégias para atendimento ao SIL requerido, tendo como premissa que a técnica de diagrama de blocos de confiabilidade será utilizada para o cálculo da PFD do sistema considerado. Estas estratégias envolvem a questão do intervalo entre testes dos sistemas de segurança e a utilização de testes parciais de elementos da FIS e redundância/configurações alternativas, entre outras, conforme apresentado a seguir.

### (A) Intervalo entre Testes dos Sistemas de Segurança

Dado as características dos equipamentos segurança, todo equipamento de proteção deve ser regularmente testado ou pode não atuar quando necessário. O teste deve ser o mais completo possível e simular condições reais, ou seja, todos os componentes do sistema de segurança (sensores, lógica e elementos finais) devem ser inspecionados e testados periodicamente para manter a integridade do sistema e estes testes devem ser extensivamente documentados (BECKMAN & CAPECCHI 2002).

As normas modernas relacionadas aos SIS sugerem cálculos para determinar o período entre testes sucessivos de uma instalação e isso faz parte do cálculo final do SIL pretendido. O problema surge na hora de testar os elementos finais. A única maneira de saber se uma válvula de *shutdown* realmente está em boas condições de atuação, e que provavelmente vai mesmo fechar em caso de necessidade, é comandar a válvula para fechar e aguardar seu fechamento total. Infelizmente, é muito caro fazer isso sem causar (ou aproveitar) uma parada de produção. Resultado estatístico: o elemento menos confiável de um sistema de *shutdown* é a válvula de *shutdown*, que, após longos períodos de inatividade, pode estar emperrada e não funcionar no momento em que é imprescindível para evitar um acidente (BEGA et al. 2003).

A Figura 6.3, busca representar este conflito entre as questões técnicas, que visam testar os sistemas de forma a manter a confiabilidade requerida e evitar acidentes, e a questão gerencial, sobre o impacto negativo de paradas de produção forçadas.


FIGURA 6.3: Freqüência de Testes

### (B) Redundância e Configurações Alternativas

Existem muitas formas de arranjar componentes de um sistema quando da cons-

trução do mesmo. Alguns arranjos são projetados para maximizar a probabilidade de sucesso da operação (confiabilidade ou disponibilidade). Alguns arranjos são projetados para minimizar a probabilidade de falha com saídas energizadas. Alguns arranjos são projetados para minimizar a probabilidade de falha com saídas desenergizadas. Outros são projetados para proteger contra outros modos de falha específicos. Estes vários arranjos dos componentes dos sistemas de controle são referenciados como "arquiteturas do sistema".

Desta forma, é possível definir "arquiteturas" como configurações específicas de elementos de *hardware* e *software* num sistema. A seleção da arquitetura tem um impacto não somente na integridade de segurança do sistema (SIL), mas também influencia diretamente a disponibilidade da planta.

A primeira preocupação do projetista é que o sistema a ser projetado seja capaz de cumprir as exigências funcionais especificadas pelo cliente ou pela companhia. Todo projetista tem conhecimento de que, em geral, há várias maneiras de se projetar um sistema para atender a uma dada função. A imposição de exigências de confiabilidade, geralmente, contribui no sentido de diminuir a gama de alternativas. Ou seja, quando são impostas exigências de confiabilidade sobre o sistema, o projetista deve proceder a uma cuidadosa busca de projetos alternativos, pois a prática mostra que sistemas projetados segundo os mesmos critérios de funcionalidade de segurança podem possuir atributos de confiabilidade que variam por ordens de magnitude.

Muitos sistemas são projetados com o uso de equipamentos redundantes. Redundância é uma técnica usada para aumentar a confiabilidade de sistemas, sem nenhuma mudança na confiabilidade das unidades individuais que o formam. Tal técnica consiste no uso de um ou mais componentes adicionais, similares ou não, de modo a se efetuar a mesma função do componente inicialmente existente. Há diferentes tipos de redundância: ativa, reserva ou k-de-n unidades, uniforme ou diversa, etc. Cada qual tem suas vantagens e desvantagens. O uso de redundância tem como objetivo aumentar a confiabilidade do sistema como um todo. Uma atenção cuidadosa é dada à escolha do tipo de redundância a ser usada, de modo a melhorar a confiabilidade global do sistema pela consideração de vários fatores (SANT´ANA 2006). A Figura 6.4 apresenta por exemplo, diferentes arranjos para válvulas.

O critério importante para a tomada de decisão em relação à forma de se usarem

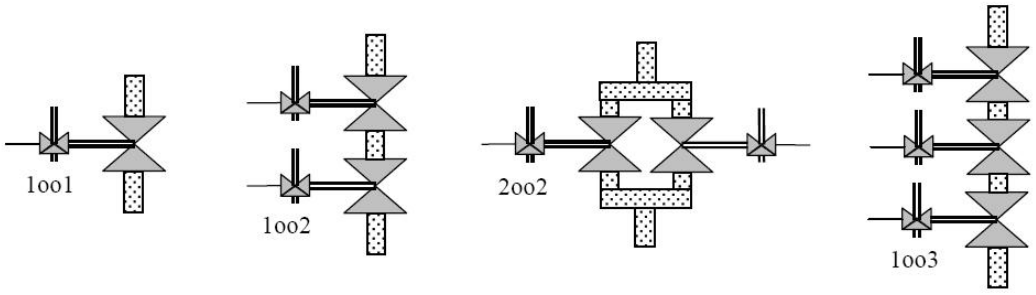


FIGURA 6.4: Exemplos de Arranjos de Válvulas

redundâncias é a relação entre confiabilidade dos subsistemas e a do sistema como um todo.

Melhorar a confiança nos elementos primários e na lógica, usando redundâncias as mais variadas, é relativamente fácil. Há, pelo menos, umas 10 tecnologias diferentes e um sem número de formas de implementá-las. Escolher as melhores alternativas para implementar um determinado sistema de segurança é que não é tão trivial. O mais delicado na prática, ainda é garantir a correta atuação do elemento final quando necessário. Este é ainda, sem dúvida, o ponto mais fraco dos sistemas (BEGA et al. 2003).

Um Sistema Instrumentado de Segurança, SIS, pode ter diferentes níveis de redundância em qualquer um dos seus três componentes básicos, possibilitando um grande número de configurações alternativas. Assim, qualquer dos três componentes básicos pode ser configurado com uma lógica do tipo k-de-n, ou seja, a ação é executada quando pelo menos k dos n componentes existentes comandam a execução da ação. As configurações mais encontradas em aplicações práticas na indústria são as do tipo 1oo1, 1oo2 e 2oo3, mas outros tipos como 2oo2 e 1oo3 são também utilizadas em aplicações especiais. Recentemente, um novo CLP foi lançado no mercado com uma configuração do tipo 2oo4, o qual, segundo seu fabricante apresenta alto nível de confiabilidade tanto para falhas críticas como para falhas espúrias (CHAME et al. 2007). Outras tecnologias de redundância existem, mas não são tão usuais nas indústrias mais comuns. Encontram-se, por exemplo, votações 2oo4, 3oo4, 4oo5 e outras em indústrias extremamente críticas, como nuclear, aeroespacial e militar.

Para aplicações SIL 2 e SIL 3, entrada dupla/tripla e saídas duplas são freqüentemente requeridas a fim de atingir a PFD média e as exigências de tolerância a falhas.

O conceito de utilizar dois ou três dispositivos para fazer exatamente o mesmo trabalho que um pode fazer é algo difícil de ser aceito. Claro, é possível projetar uma FIS completamente simples que atinja um valor alto de SIL, mas o intervalo entre testes requerido é tipicamente intolerável para a equipe de manutenção. Para SIL 2 ou SIL 3, baixa redundância geralmente requer testes *on line*, enquanto que alta redundância pode estender o intervalo entre testes para as paradas das unidades (*turnaround*).

Finalmente, a arquitetura de votação pode impactar na taxa de falha espúria da FIS. Dispositivos únicos podem atingir o SIL a baixo custo de capital e custo de instalação. A FIS pode também ter uma alta taxa de falha espúria, que freqüentemente causa uma substancial perda de produção. Alternativas de projeto podem ser redundantes para garantir tolerância a falhas. Isto pode aumentar o custo de instalação, mas irá diminuir substancialmente a taxa de falha espúria.

### (C) Testes Parciais dos Sistemas de Segurança

Conforme citado, dadas as características dos equipamentos de segurança, todo equipamento de proteção deve ser regularmente testado ou pode não atuar quando necessário. O teste deve ser completo (o mais possível) e simular condições reais. No entanto, testes parciais podem ser utilizados para complementar os testes totais do sistema com o intuito de reduzir a probabilidade de falha na demanda do mesmo sem necessidade de parada da planta para a sua realização.

Conforme (SUMMERS & ZACHARY 2002), existem diversos métodos para a realização de testes parciais disponíveis para o usuário. Cada método apresenta diferentes componentes para facilitar o teste e deve ser avaliado individualmente para a verificação do seu impacto específico para o SIL do sistema de segurança. Outro ponto a destacar é que, dado que os testes são realizados automaticamente pelo sistema, custos com mão-de-obra são minimizados, permitindo em muitos casos, atingir o SIL requerido sem causar impactos nos custos de manutenção e operação.

É visível pelos dados disponíveis na literatura (por exemplo, no OREDA (OREDA 2002)), que a maior proporção de falhas não detectadas são relacionadas aos elementos finais, por exemplo, uma válvula de *shutdown*. Um teste parcial desta válvula pode ser definido como: permitir ao sistema de segurança fechar a válvula somente 20%.

Neste caso, todos os elementos estariam sendo testados, entretanto a válvula nunca fecha completamente durante o teste.

## 6.5 Alternativas Consideradas

Esta seção tem como objetivo apresentar e detalhar as alternativas que serão consideradas para a realização da análise custo-benefício que busca encontrar a melhor configuração do sistema de bloqueio do refervedor, de modo que o mesmo atenda ao requisito de SIL 3, conforme explicado na seção anterior.

Cabe ressaltar que cada alternativa, ou função instrumentada de segurança (FIS), é composta por iniciador, executor da lógica e atuador. Este estudo propõe a análise de dez alternativas para a FIS do sistema de bloqueio do refervedor. Todas estas alternativas envolvem diferentes configurações (as mais usuais na indústria de processos) dos seguintes componentes: transmissores de pressão, CLPs e válvulas de bloqueio.

Transmissores podem ser entendidos como instrumentos que convertem o sinal de um transdutor ou sensor em um sinal padrão para ser enviado à distância. Basicamente, os transmissores de pressão podem ser classificados em pneumáticos ou eletrônicos. Os dois tipos de transmissores baseiam seu funcionamento no movimento/deformação que os elementos mecânicos elásticos (deformação de sólidos) sofrem submetidos a uma pressão/esforço. Este movimento/deformação, que é proporcional à pressão aplicada (Lei de Hooke), é convertido através de um transdutor, em um sinal pneumático ou eletrônico padronizado, que é enviado/transmitido para indicação e/ou controle à distância (BEGA et al. 2003).

O Controlador Lógico Programável (CLP ou PLC, do inglês, *Programmable Logic Controller*), é um equipamento de controle industrial microprocessado, criado inicialmente para efetuar especificamente o controle lógico de variáveis discretas, e atualmente é usado para praticamente todos os tipos de controle. O CLP funciona seqüencialmente, olhando o estado dos dispositivos ligados às suas entradas, operando a lógica de seu programa interno e determinando o estado dos dispositivos ligados às suas saídas (BEGA et al. 2003). Os CLPs podem apresentar diversas configurações, conhecidas como simplex, dual-simplex, dual-dual, triplex (com votação 2oo3) e até mesmo uma configuração do tipo 2oo4, lançada recentemente no mercado, e que, segundo seu fa-

bricante apresenta alto nível de confiabilidade, tanto para falhas críticas como para falhas espúrias. Embora a configuração mais utilizada na indústria petroquímica seja a dual-simplex, ou "hot standby", neste trabalho, as alternativas mais básicas que serão analisadas, consideram o CLP simplex (caracterizada por uma única unidade de processamento (CPU) que funciona ativamente no controle do sistema) e as demais, o CLP *hot standby* (caracterizado pela duplicação das unidades de processamento (CPU´s) dispostas em uma arquitetura que permite o compartilhamento das unidades de entrada e saída; uma CPU é mantida ativa e controla o sistema, a outra serve de unidade "back up" em caso de falha da unidade ativa).

Válvulas de bloqueio são responsáveis pela manipulação do fluxo de matéria e/ou energia, que têm como finalidade atuar no processo de modo a corrigir o valor da variável controlada sempre que houver algum desvio em relação ao valor desejado. Dois tipos de válvulas serão consideradas para as alternativas selecionadas: válvula de bloqueio com sua válvula solenóide associada (aqui denominada "Válvula de Bloqueio Tipo 1") e válvula de bloqueio com posicionador que permite a realização de testes parciais (aqui denominada"Válvula de Bloqueio Tipo 2"). Tanto a válvula solenóide quanto o posicionador são acessórios comumente utilizados em conjunto com as válvulas de bloqueio, cujas funções dependem da necessidade do processo. Conforme cita Koch (BEGA et al. 2003), as válvulas solenóides, quando utilizadas em conjunto com as válvulas de bloqueio, exercem a função de piloto ou comando, fazendo com que o ar de comando passe para o atuador, ou desvie do atuador para a atmosfera, abrindo ou fechando a válvula; e o posicionador é um servo-amplificador cuja função é assegurar o correto posicionamento da haste da válvula, de acordo com o sinal de comando correspondente, enviado pelo controlador.

Os posicionadores, a exemplo da maioria dos transmissores eletrônicos atuais, são hoje, em sua maioria inteligentes. São baseados em microprocessadores, que apresentam um sinal digital de comunicação superposto ao sinal analógico de transmissão de 4-20mA CC, permitindo o intercâmbio de informações com a sala de controle, de forma a executar uma série de funções adicionais de que um sistema convencional não dispõe. Assim, os posicionadores inteligentes podem ser ligados em rede, possibilitando calibração remota a partir da sala de controle, monitoração da posição da válvula a cada instante, verificação da correspondência da real posição da haste em relação ao sinal

proveniente do controlador, diagnósticos de falhas e outras (BEGA et al. 2003).

Conforme citado na seção anterior, a alternativa mais básica proposta para o sistema consiste de um único transmissor de pressão, a unidade lógica (CLP) do tipo simplex e uma única válvula de bloqueio (com a sua válvula solenóide associada). Esta é a configuração representada na Figura 6.2 e apresentada na Figura 6.5. Um grande número de outras configurações são possíveis e as selecionadas para análise neste estudo, estão apresentadas na Tabela 6.1. Conforme destacado, cada FIS, é composta pelo iniciador, pelo executor da lógica e pelo atuador e é desta forma que elas estão apresentadas na referida tabela. Outro ponto a destacar, é que o dado apresentado entre parênteses indica a lógica de votação dentro de cada um dos grupos de componentes.

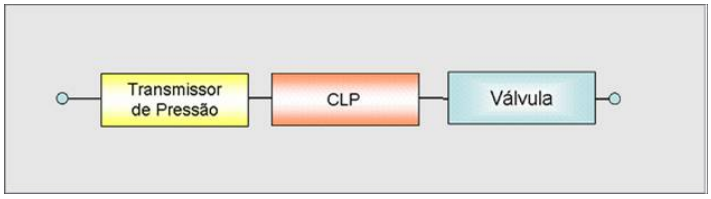


FIGURA 6.5: Configuração Básica da Função Instrumentada de Segurança

Analisando a Tabela 6.1, é possível verificar que as dez alternativas analisadas podem ser divididas em dois grandes grupos. O primeiro, contém as alternativas denominadas "FIS A-1" até "FIS E-1", sendo o número "1" representativo da presença da válvula de bloqueio tipo 1 nas configurações; o segundo grupo contém as alternativas denominadas "FIS A-2" até "FIS E-2", sendo o número "2" representativo da presença da válvula de bloqueio tipo 2 nas configurações.

É possível observar também, pelos dados apresentados na Tabela 6.1, que as alternativas consideradas estão relacionadas a diferentes configurações do sistema (redundância) e à utilização de testes parciais do elemento final entre os períodos de teste total do sistema. Vale lembrar que testes parciais podem ser utilizados para complementar os testes totais do sistema com o intuito de reduzir a probabilidade de falha na demanda do mesmo, sem necessidade de parada da unidade para a sua realização.

Tabela 6.1: Alternativas Consideradas

| Alternativa | Iniciador | Lógica | Atuador |
|---|---|---|---|
| FIS A-1 | Transmissor de Pressão (1oo1) | CLP (1oo1) | Válvula de Bloqueio Tipo 1* (1oo1) |
| FIS B-1 | Transmissor de Pressão (1oo1) | CLP hot standby (1oo2) | Válvula de Bloqueio Tipo 1* (1oo1) |
| FIS C-1 | Transmissor de Pressão (1oo1) | CLP hot standby (1oo2) | Válvula de Bloqueio Tipo 1* (1oo2) |
| FIS D-1 | Transmissor de Pressão (1oo2) | CLP hot standby (1oo2) | Válvula de Bloqueio Tipo 1* (1oo2) |
| FIS E-1 | Transmissor de Pressão (2oo3) | CLP hot standby (1oo2) | Válvula de Bloqueio Tipo 1* (1oo2) |
| FIS A-2 | Transmissor de Pressão (1oo1) | CLP (1oo1) | Válvula de Bloqueio Tipo 2* (1oo1) |
| FIS B-2 | Transmissor de Pressão (1oo1) | CLP hot standby (1oo2) | Válvula de Bloqueio Tipo 2* (1oo1) |
| FIS C-2 | Transmissor de Pressão (1oo1) | CLP hot standby (1oo2) | Válvula de Bloqueio Tipo 2* (1oo2) |
| FIS D-2 | Transmissor de Pressão (1oo2) | CLP hot standby (1oo2) | Válvula de Bloqueio Tipo 2* (1oo2) |
| FIS E-2 | Transmissor de Pressão (2oo3) | CLP hot standby (1oo2) | Válvula de Bloqueio Tipo 2* (1oo2) |



(*) Tipo 1 = Válvula de bloqueio com solenóide
(**) Tipo 2 = Válvula de bloqueio com posicionador que permite a realização de testes parciais

## 6.6 Apresentação dos Dados para Análise e Premissas Consideradas

Na realização de uma avaliação quantitativa em um estudo de confiabilidade, um elemento de fundamental importância é o conhecimento dos chamados dados de falhas (ou de confiabilidade). É possível dizer que existem três fontes básicas de dados de confiabilidade que podem ser utilizados, sendo que cada uma destas fontes possui suas próprias vantagens e desvantagens, no entanto, a discussão detalhada destes tópicos não faz parte do escopo do presente trabalho. A primeira fonte pode ser descrita como dados específicos da unidade (avaliação do desempenho do componente com o tempo, numa aplicação e em um ambiente semelhante). A segunda grande fonte de dados de confiabilidade de equipamentos, são os bancos de dados publicados pela indústria. Conforme citado na seção 2.3.2.1, há uma grande diversidade de literatura a respeito, como OREDA (*Offshore Reliability Database*) e SINTEF, disponíveis aos usuários. A terceira fonte de dados e a mais detalhada é uma Análise de Modos de Falhas, Efeitos e Diagnósticos (*Failure Modes, Effects and Diagnostic Analysis* - FMEDA) do equipamento.

Para a verificação do nível do integridade de segurança de *hardware*, de acordo com a Norma IEC 61508, somente falhas randômicas de equipamentos são de interesse para a análise do cálculo da PFD. Neste tipo de análise, considera-se que o equipamento foi propriamente selecionado para a aplicação e adequadamente comissionado. A Norma assume o modelo de taxa de falha constante e requer uma estimativa da taxa de falha de cada componente. Esta estimativa pode ser feita tanto por meio de uma análise quantitativa de modo de falhas do projeto do equipamento ou a partir da experiência de um uso prévio do equipamento (do inglês, "proven in use"). Para validar os dados baseados nesta última opção, uma série de exigências têm que ser consideradas e estão listadas na referida norma.

As Tabelas 6.2 e 6.3 apresentam os dados utilizados para a avaliação do sistema, sendo que a primeira delas apresenta dados extraídos do banco de dados do SINTEF (HAUGE, LANGSETH & ONSHUS 2006), e o segundo, valores típicos da indústria de processos, adotados como premissas para o estudo.

A Tabela 6.2 possui cinco colunas, que seqüencialmente apresentam: o elemento da

FIS cujos dados serão apresentados; a taxa de falha crítica (ou perigosa, "dangerous failure rate"), $\lambda_D$; a taxa de falha espúria (ou segura, "spurious failure rate"), $\lambda_S$; o fator de cobertura do diagnóstico, DC, denominado "diagnostic coverage" e o fator beta para falhas perigosas não-detectadas, $\beta$.

TABELA 6.2: Dados utilizados na análise - Fonte SINTEF

| Equipamento | $\lambda_D(/h)$ | $\lambda_S(/h)$ | DC | $\beta$ |
|---|---|---|---|---|
| Transmissor de Pressão | 0,80E-06 | 0,50E-06 | 0,60 | 0,03 |
| CLP simplex | 1,00E-06 | 1,00E-06 | 0,90 | 0,02 |
| Válvula Tipo 1 | 4,00E-06 | 4,60E-06 | 0,30 | 0,02 |
| Válvula Tipo 2 | 2,70E-06 | 2,70E-06 | 0,25 | 0,02 |

A Tabela 6.3 possui quatro colunas, que seqüencialmente apresentam: o elemento da FIS cujos dados serão apresentados; o tempo médio até a restauração da função do componente, canal ou sistema (MTTR, do inglês, "Mean Time to Restoration", de acordo com as Normas IEC 61508 e 61511, referenciadas neste trabalho); o MTTR espúrio, ou seja, o tempo médio até a restauração da função do componente, canal ou sistema devido a uma falha espúria; e, finalmente, o custo em dólares referente ao valor necessário de investimento para a compra de cada um dos elementos da FIS.

TABELA 6.3: Dados utilizados na análise - Fonte Indústria

| Equipamento | MTTR (h) | MTTR esp. (h) | Custo (US$) |
|---|---|---|---|
| Transmissor de Pressão | 8 | 6 | 1,000 |
| CLP simplex | 4 | 4 | 25,000 (*) |
| Válvula Tipo 1 | 24 | 5 | 15,000 |
| Válvula Tipo 2 | 24 | 5 | 20,000 |

(*) O Custo estimado do CLP *hot standby* é de US$ 40,000

Para a análise das alternativas propostas para o sistema de bloqueio para proteção do *header* do flare, foi necessário fazer algumas considerações e adotar algumas premissas, as quais estão listadas abaixo:

- A política de manutenção da empresa em análise consiste em realizar uma parada geral de toda a unidade a cada cinco anos, quando então são feitos testes completos nos sistemas de proteção.

- Para se testar o sistema em análise, em qualquer momento que não na parada programada, são necessárias quatro horas de parada da planta, sendo uma hora referente ao tempo necessário para a realização do teste e três horas necessárias para trazer a planta de volta à operação normal. Para fins desta análise, considerou-se que a empresa incorre em uma "perda de produção" igual a US$20,000 por hora parada, de modo que cada teste acarreta uma perda total de US$80,000.

- Além dos custos associados à parada de produção, não serão considerados os custos para a realização de testes parciais, pois assumiu-se que estes custos são muito pequenos, dado que envolvem somente custo de mão de obra, são feitos rapidamente, e não envolvem perda de produção.

- Para as alternativas que utilizam a válvula de bloqueio do tipo 2 (dotada de posicionador que permite a realização de testes parciais), considerou-se um coeficiente de diagnóstico de teste parcial igual a 0,8 para $\lambda_D$, ou seja, 80% das falhas críticas são detectadas durante a realização de um teste parcial neste componente.

- A periodicidade proposta de testes parciais para a(s) válvula(s) do tipo 2 é de 15 dias (360 horas).

- Seguindo uma orientação da Norma IEC 61508, foi considerado para o cálculo da PFD, que o valor de $\beta_D$, fator $\beta$ para falhas detectadas (ou seja, percentual da taxa de falha total detectada do componente que pode ser considerada como falha de modo comum detectada), corresponde a 50% do valor de $\beta$ (percentual da taxa de falha total não detectada do componente que pode ser considerada como falha de causa comum não detectada).

## 6.7 Resultados Obtidos para as Alternativas Selecionadas

Esta seção objetiva apresentar os resultados da análise custo-benefício das alternativas propostas para que o sistema de bloqueio do refervedor para proteção do *header* do flare de uma grande empresa petroquímica atenda a um requisito de confiabilidade SIL

3. Em relação aos resultados obtidos para cada uma das dez alternativas analisadas, serão apresentados nas seções a seguir:

- Custo da aquisição dos equipamentos da FIS;
- Cálculo da PFD para intervalos de testes variando desde 1 mês até 5 anos;
- Valor máximo do intervalo entre testes;
- Número mínimo de paradas da unidade por ano para teste da FIS;
- Custo anual devido a paradas para testes da FIS;
- Número de paradas anuais devido a falhas espúrias dos equipamentos da FIS;
- Custo anual devido a paradas espúrias;
- Custo do Ciclo de Vida da FIS.

### 6.7.1 Cálculo da Probabilidade de Falha na Demanda (PFD)

Conforme citado anteriormente, a PFD pode ser definida como um atributo de confiabilidade que indica qual a probabilidade de um componente falhar em cumprir uma ação previamente especificada no momento em que ela for demandada e deve ser calculada para a verificação do atendimento ao requisito mínimo de PFD decorrente da premissa de requerimento SIL 3.

Esta seção apresenta os resultados do cálculo da PFD das alternativas analisadas para a avaliação custo-benefício, escopo deste estudo. O cálculo da PFD para funções instrumentadas de segurança foi detalhado no Capítulo 5 deste trabalho e deve ser consultado em caso de necessidade de esclarecimentos adicionais. Cabe ressaltar que estes cálculos foram realizados com o auxílio do *software* ORBIT SIL (CHAME & OLIVEIRA 2006), desenvolvido pela DNV (Det Norske Veritas) para a análise de integridade de funções instrumentadas de segurança.

A Tabela 6.4 apresenta os resultados para as dez alternativas analisadas, considerando intervalos entre testes completos de 1 mês, 3 meses, 6 meses, 1 ano, 2 anos, 3 anos e 5 anos. Para cada uma das alternativas, é apresentado o valor da PFD para o intervalo entre testes correspondente e o SIL correspondente a este valor de PFD.

Tabela 6.4: Intervalo entre Testes para cada Alternativa analisada

| | | Intervalo entre Testes | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Alternativa | | 1 mês | 3 meses | 6 meses | 1 ano | 2 anos | 3 anos | 5 anos |
| FIS A-1 | PFD | 1,27E-03 | 3,58E-03 | 7,16E-03 | 1,42E-02 | 2,83E-02 | 4,24E-02 | 7,06E-02 |
| | SIL | SIL 2 | SIL 2 | SIL 2 | SIL 1 | SIL 1 | SIL 1 | SIL 1 |
| FIS B-1 | PFD | 1,23E-03 | 3,47E-03 | 6,94E-03 | 1,38E-02 | 2,75E-02 | 4,11E-02 | 6,85E-02 |
| | SIL | SIL 2 | SIL 2 | SIL 2 | SIL 1 | SIL 1 | SIL 1 | SIL 1 |
| FIS C-1 | PFD | 1,46E-04 | 4,29E-04 | 8,86E-04 | 1,86E-03 | 4,10E-03 | 6,73E-03 | 1,32E-02 |
| | SIL | SIL 3 | SIL 3 | SIL 3 | SIL 2 | SIL 2 | SIL 2 | SIL 1 |
| FIS D-1 | PFD | 2,780E-05 | 8,77E-05 | 2,01E-04 | 4,98E-04 | 1,39E-03 | 2,67E-03 | 6,41E-03 |
| | SIL | SIL 4 | SIL 4 | SIL 3 | SIL 3 | SIL 2 | SIL 2 | SIL 2 |
| FIS E-1 | PFD | 2,784E-05 | 8,80E-05 | 2,02E-04 | 5,03E-04 | 1,41E-03 | 2,72E-03 | 6,54E-03 |
| | SIL | SIL 4 | SIL 4 | SIL 3 | SIL 3 | SIL 2 | SIL 2 | SIL 2 |
| FIS A-2 | PFD | 6,64E-04 | 1,26E-03 | 2,17E-03 | 3,98E-03 | 7,59E-03 | 1,12E-02 | 1,84E-02 |
| | SIL | SIL 3 | SIL 2 | SIL 2 | SIL 2 | SIL 2 | SIL 1 | SIL 1 |
| FIS B-2 | PFD | 6,25E-04 | 1,15E-03 | 1,96E-03 | 3,55E-03 | 6,73E-03 | 9,92E-03 | 1,63E-02 |
| | SIL | SIL 3 | SIL 2 | SIL 2 | SIL 2 | SIL 2 | SIL 2 | SIL 1 |
| FIS C-2 | PFD | 1,33E-04 | 3,71E-04 | 7,38E-04 | 1,47E-03 | 2,93E-03 | 4,39E-03 | 7,36E-03 |
| | SIL | SIL 3 | SIL 3 | SIL 3 | SIL 2 | SIL 2 | SIL 2 | SIL 2 |
| FIS D-2 | PFD | 1,460E-05 (*) | 2,94E-05 | 5,30E-05 | 1,02E-04 | 2,11E-04 | 3,33E-04 | 6,18E-04 |
| | SIL | SIL 4 | SIL 4 | SIL 4 | SIL 3 | SIL 3 | SIL 3 | SIL 3 |
| FIS E-2 | PFD | 1,464E-05 (*) | 2,98E-05 | 5,43E-05 | 1,07E-04 | 2,31E-04 | 3,78E-04 | 7,44E-04 |
| | SIL | SIL 4 | SIL 4 | SIL 4 | SIL 3 | SIL 3 | SIL 3 | SIL 3 |

(*) Maior número de casas decimais para poder facilitar a visualização da diferença.

Conforme citado na seção 6.5 deste capítulo, as alternativas analisadas podem ser divididas em dois grandes grupos: o **Grupo 1**, contendo as alternativas denominadas "FIS A-1" até "FIS E-1", sendo o número "1" representativo da presença da válvula de bloqueio tipo 1 nas configurações; e o segundo, **Grupo 2**, contendo as alternativas denominadas "FIS A-2" até "FIS E-2", sendo o número "2" representativo da presença da válvula de bloqueio tipo 2 nas configurações.

De forma a facilitar a visualização dos resultados apresentados na Tabela 6.4, os mesmos serão representados em termos gráficos e apresentados em três figuras deste ponto em diante. A Figura 6.6, apresenta a variação do valor da PFD em função do intervalo entre testes para as alternativas do Grupo 1, a Figura 6.7, apresenta este mesmo gráfico para os resultados do Grupo 2, e a Figura 6.8, apresenta o resultado geral contemplando todas as alternativas consideradas (Grupo 1 e Grupo 2).

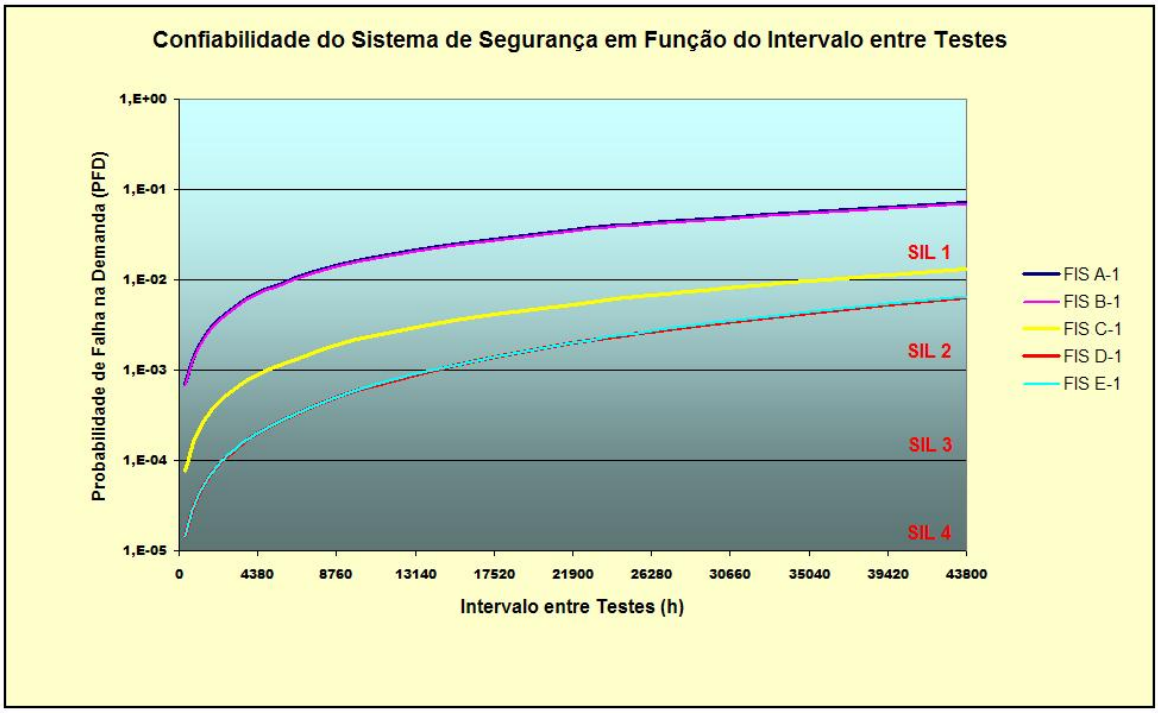


FIGURA 6.6: PFD em função do Intervalo entre Testes para o Grupo 1

Conforme citado, a Figura 6.6 representa os resultados apresentados na Tabela 6.4, para as alternativas do Grupo 1, sob a forma gráfica. Analisando os resultados, é possível verificar que as alternativas FIS A-1 e FIS B-1 apresentam resultados muito próximos, o que torna dificilmente possível a distinção de suas curvas na figura. O mesmo raciocínio vale para as alternativas FIS D-1 e FIS E-1.

A visualização gráfica permite identificar o comportamento do valor da PFD com o tempo para cada uma das alternativas, e as marcações horizontais que delimitam as faixas de valores característicos de cada SIL, auxiliando a verificação dos pontos (intervalos máximos de tempo entre testes) correspondentes a cada valor de SIL. Por exemplo, para a alternativa FIS C-1, é possível visualizar que ela atende a SIL 3 para um intervalo de teste máximo de aproximadamente 4380 horas (o valor exato já foi calculado e está apresentado na Tabela 6.5), que atende a SIL 2, deste ponto até aproximadamente 35040 horas (4 anos), e SIL 1 deste ponto em diante até um determinado valor de intervalo entre testes que não está visualisado no gráfico.

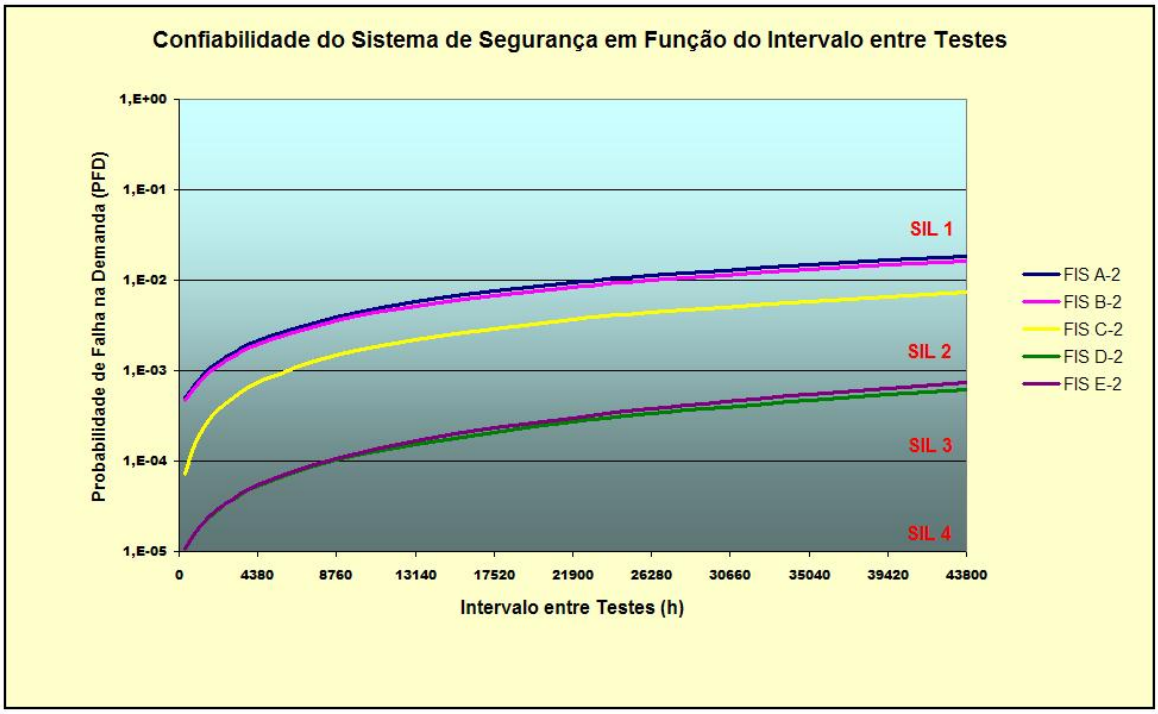


FIGURA 6.7: PFD em função do Intervalo entre Testes para o Grupo 2

Conforme citado, a Figura 6.7 representa os resultados apresentados na Tabela 6.4, para as alternativas do Grupo 2, sob a forma gráfica. Analisando os resultados, é possível verificar que, as alternativas FIS A-2 e FIS B-2, apresentam resultados muito próximos, no entanto, a pequena distinção de suas curvas na figura é um pouco mais visível. O mesmo raciocínio vale para as alternativas FIS D-2 e FIS E-2.

Da Figura 6.7, vê-se que para a alternativa FIS C-2, é possível visualizar que ela atende a SIL 3 para um intervalo de teste máximo de aproximadamente 6000 horas (o valor exato já foi calculado e está apresentado na Tabela 6.5), e a SIL 2, deste ponto

em diante até um determinado valor de intervalo entre testes que não está visualisado no gráfico.

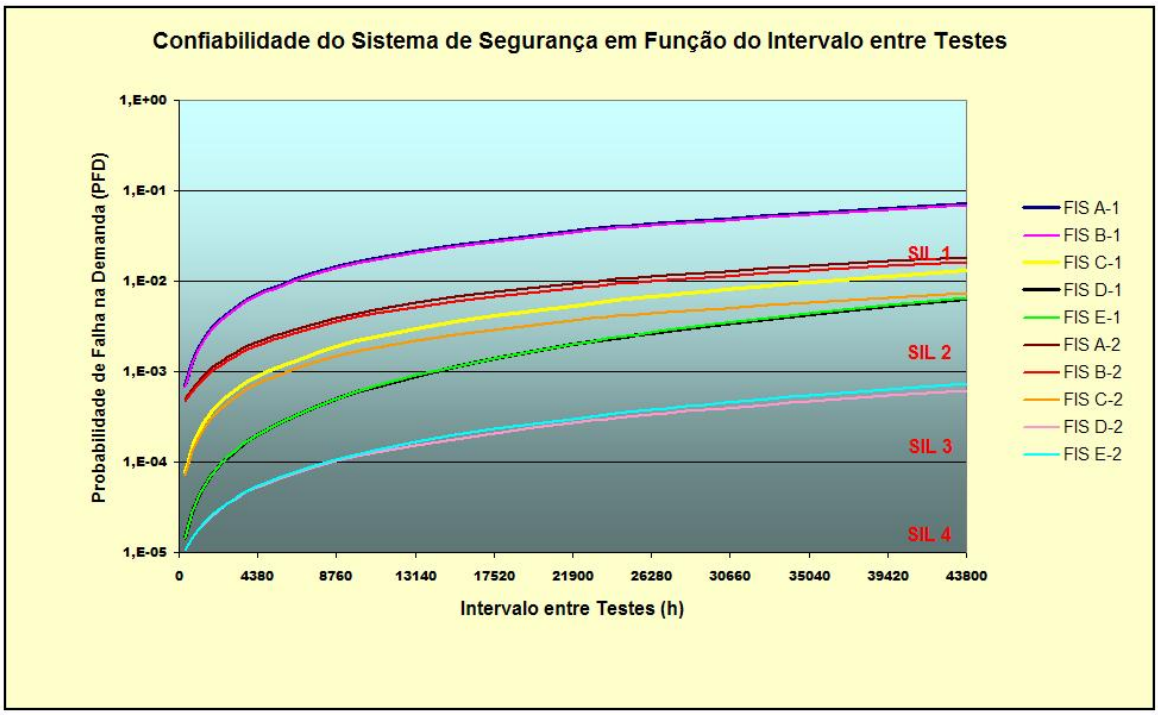


FIGURA 6.8: PFD em Função do Intervalo entre Testes

Conforme citado, a Figura 6.8 representa os resultados apresentados na Tabela 6.4 para todas as configurações analisadas, sob a forma gráfica. Analisando os resultados, é possível verificar que, as alternativas FIS D-2 e FIS E-2, apresentam os melhores resultados em termos de PFD e que eles são muito próximos. O mesmo raciocínio vale para as alternativas FIS A-1 e FIS B-1, que apresentam os piores resultados em termos de PFD e também são muito próximos.

Cabe destacar novamente que o máximo valor do intervalo entre testes da FIS que garante o atendimento ao SIL 3 requerido, para cada uma das dez alternativas analisadas, está apresentado na Tabela 6.5. Esses valores máximos para cada configuração, correspondem aos pontos de interseção entre as respectivas curvas e a linha horizontal de $10^{-3}$ da PFD da Figura 6.8.

A Tabela 6.5 contém quatro colunas, que seqüencialmente apresentam: a alternativa que está sendo analisada; o máximo valor de intervalo entre testes totais do sistema (em horas) que garante o atendimento ao requisito SIL 3; este mesmo valor máximo expresso em termos anuais, e finalmente o número mínimos de paradas por ano para

testes totais da FIS, para cada uma das alternativas selecionadas.

Tabela 6.5: Intervalo de Testes para atendimento a SIL 3

| Alternativa | Máximo Intervalo Testes (h) | Máximo Intervalo Testes (anos) | Número Mínimo paradas/ano |
|---|---|---|---|
| FIS A-1 | 555 | 0,063 | 15,783 |
| FIS B-1 | 575 | 0,066 | 15,235 |
| FIS C-1 | 4914 | 0,561 | 1,783 |
| FIS D-1 | 14158 | 1,616 | 0,619 |
| FIS E-1 | 14036 | 1,602 | 0,624 |
| FIS A-2 | 1535 | 0,175 | 5,707 |
| FIS B-2 | 1753 | 0,200 | 4,998 |
| FIS C-2 | 5957 | 0,680 | 1,471 |
| FIS D-2 | 63345 | 7,231 | 0,138 |
| FIS E-2 | 54004 | 6,165 | 0,162 |

É possível verificar pelos resultados apresentados na Tabela 6.5, que as alternativas "FIS D-2" e "FIS E-2" são as que permitem os maiores valores de intervalo entre testes totais do sistema dado o requisito de atendimento a SIL 3, aproximadamente 7 e 6 anos, respectivamente. Cabe destacar que estes valores, são inclusive maiores do que o intervalo programado de parada da unidade, de acordo com a política de parada programada da empresa (ver seção 6.6), que é de 5 anos. Desta forma, pelo menos a cada 5 anos, estas funções serão testadas, ou seja, é possível admitir que o máximo intervalo entre testes dos sistemas, será a cada 5 anos. Embora fique claro que o sistema poderia ser testado em um intervalo de testes maior do que o de parada programada da unidade, deste ponto em diante, será considerado que este é o intervalo máximo de testes a que as alternativas "FIS D-2" e "FIS E-2" estarão sujeitas. Cabe destacar que esta é uma premissa conservativa, cujas conseqüências serão analisadas adiante neste trabalho.

A Tabela 6.6 apresenta a alteração proposta no parágrafo anterior para as alternativas "FIS D-2" e "FIS E-2", que serão denominadas deste ponto em diante como "FIS D-2*" e "FIS E-2*".

TABELA 6.6: Intervalo Testes para SIL 3 - Considerando Parada Programada

| Alternativa | Máximo Intervalo Testes (h) | Máximo Intervalo Testes (anos) | Número Mínimo paradas/ano |
|---|---|---|---|
| FIS D-2* | 43800 | 5,000 | 0,200 |
| FIS E-2* | 43800 | 5,000 | 0,200 |

### 6.7.2 Cálculo do Custo do Ciclo de Vida (CCV)

Conforme citado anteriormente, o Custo do Ciclo de Vida (CCV) pode ser entendido como uma ferramenta de gestão que visa ajudar a minimização de custos e a maximização do rendimento para variados tipos de sistemas. A determinação do CCV é um método que permite a comparação de soluções alternativas, em termos de custos. Trata-se basicamente de um processo matemático, cujo resultado é bastante dependente da informação disponível, logo, os resultados do processo apresentam certamente um grau de confiança similar ao dos dados utilizados.

O CCV de qualquer sistema é equivalente ao seu custo total durante o seu período de vida útil; no entanto, os fatores de custo que devem ser consideradas em uma análise do custo do ciclo de vida variam de sistema para sistema. No entanto, só serão consideradas as perdas econômicas de produção provocadas pela atuação indevida (desligamentos espúrios) do sistema de segurança. O método é abrangente, porém, neste caso, não serão consideradas as perdas econômicas diretas ou indiretas provocadas por acidentes resultantes da falha do sistema de segurança, tais como penalidades contratuais ou prêmios de seguro, por exemplo.

A combinação da análise de confiabilidade e o custo do ciclo de vida na escolha de alternativas de projetos é um poderoso instrumento decisório na engenharia. O CCV é um atributo econômico de significado amplo e eficaz para comparação de alternativas de projeto de um sistema. No cálculo do CCV é computado o custo de investimento (diretamente relacionado à complexidade, ou ao maior número de equipamentos), o custo de operação e manutenção e o custo de indisponibilidade (perda econômica de produção) ao longo da vida útil da unidade considerada.

O CCV não segue uma relação proporcional à complexidade (maior número de componentes) dado que uma de suas partes componentes, a perda econômica de produção,

é dependente do produto da freqüência de desligamento espúrio e do custo de produção devido ao desligamento espúrio. A freqüência de desligamento espúrio, por sua vez, é dependente do tipo de configuração escolhida e da sua política de testes, enquanto o custo da perda de produção devido ao desligamento espúrio depende também do tempo médio de retorno à produção normal.

Em termos de sistemas instrumentados de segurança (SIS), o custo do risco aumenta quando a probabilidade de falha na demanda aumenta. Enquanto o nivelamento de segurança em termos de SIL são normalmente ditatos por um estudo de risco, reduzir custos pode justificar até mesmo maiores níveis de integridade de segurança (GOBLE 1998). Ainda de acordo com GOBLE (1998), os custos do risco são calculados pela multiplicação do custo do evento multiplicado pela probabilidade do evento. Se um SIS é utilizado, a probabilidade do evento equivale à probabilidade de um evento sem o SIS vezes a PFD do SIS.

Conforme discutido anteriormente, o principal objetivo do presente trabalho é analisar possíveis alternativas para atendimento a um SIL requerido 3 para uma FIS de um sistema de bloqueio contra alta pressão em um refervedor de uma planta petroquímica, buscando minimizar o custo total ou custo do ciclo de vida para a unidade. Para tal, o CCV será calculado conforme apresentado na equação 6.1.

$$\text{Custo do Ciclo de Vida} = CAPEX + OPEX + RISKEX \tag{6.1}$$

Desta forma, é possível verificar que os fatores de custos considerados para a análise do custo do ciclo de vida deste sistema serão o **CAPEX** (*capital expenditures*), o **OPEX** (*operating expenditures*) e o **RISKEX** (*risk expenditures*).

A rentabilidade de um projeto é função de vários fatores relacionados a gastos e receitas, tais como custos de capital, custos operacionais, taxa de produção, preço do produto, freqüência de falha de equipamentos, o tempo de parada associado com estas falhas, etc. Falhas de equipamentos reduzem a receita potencial que poderia ser geradas pelo sistema e aumentam o custo operacional. Em relação ao apresentado na equação 6.1, é possível verificar que novos empreendimentos que envolvam um determinado risco sob o capital investido são avaliados com base em um balanço entre receita potencial, custos de capital (CAPEX), custo operacional (OPEX) e custo do risco (RISKEX), de

acordo com a seguinte expressão (ALVARENGA 2005):

$$\text{Lucro} = Max(Receita - CAPEX - OPEX - RISKEX) \tag{6.2}$$

Nas seções 6.7.2.1, 6.7.2.2 e 6.7.2.3, discute-se um pouco mais cada um destes parâmetros e apresentam-se os seus respectivos cálculos e resultados.

#### 6.7.2.1 Cálculo do CAPEX

Conforme citado anteriormente, um dos fatores que será considerado para o cálculo do custo do ciclo de vida das alternativas propostas para a função instrumentada de segurança do refervedor de uma unidade petroquímica, é o CAPEX (do inglês, *Capital Expenditures*), ou Custo de Capital.

De forma geral, é possível dizer que o CAPEX inclui os custos de projeto inicial, engenharia, construção e investimentos relacionados a modificações durante a vida da instalação (ERIKSEN, HARMS & MCDONNELL 1999).

Nesta análise, este custo envolve basicamente a aquisição dos equipamentos de cada uma das configurações propostas para a realização da análise custo-benefício realizada neste trabalho. Os valores referentes ao CAPEX de cada uma das alternativas propostas (ver Tabela 6.1) estão apresentados, na Tabela 6.7 e na Figura 6.9, tendo sido calculados com os dados apresentados na Tabela 6.2.

Tabela 6.7: CAPEX (em US$) por Alternativa Analisada

| Alternativa | CAPEX (US$) |
|---|---|
| FIS A-1 | 41,000 |
| FIS B-1 | 56,000 |
| FIS C-1 | 71,000 |
| FIS D-1 | 72,000 |
| FIS E-1 | 73,000 |
| FIS A-2 | 46,000 |
| FIS B-2 | 61,000 |
| FIS C-2 | 81,000 |
| FIS D-2 | 82,000 |
| FIS E-2 | 83,000 |

É possível verificar pelos resultados apresentados na Tabela 6.7 que, conforme esperado, quanto mais redundante o sistema, maior o valor do CAPEX da alternativa.

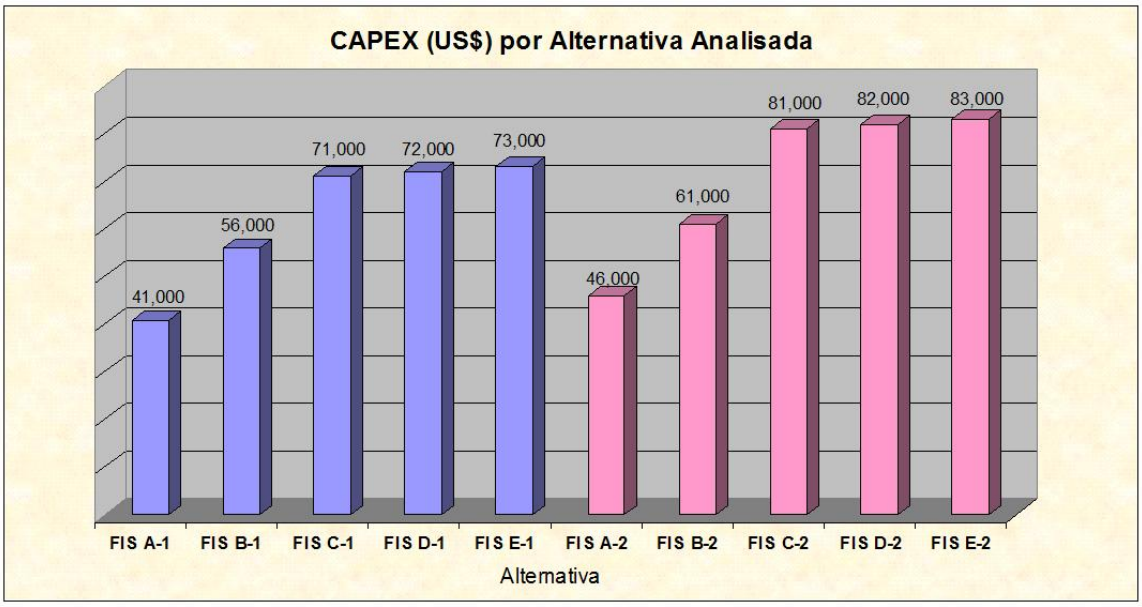


FIGURA 6.9: CAPEX (US$) por Alternativa Analisada

Assim, as alternativas FIS E-1 e FIS E-2 são as que apresentam os maiores valores de custo de aquisição de equipamentos.

#### 6.7.2.2 Cálculo do OPEX

O segundo fator considerado para o cálculo do custo do ciclo de vida das alternativas propostas para a função instrumentada de segurança do refervedor da unidade petroquímica é o OPEX (do inglês, *Operational Expenditures*), ou Custo Operacional.

O OPEX representa o custo necessário para manter o sistema operando, ou seja, este valor considera que serão realizados tantos testes quanto necessários para manter o sistema operando e em conformidade com o requisito de SIL 3, premissa deste trabalho. Portanto, para o cálculo desta parcela é necessário avaliar o número de paradas necessárias (para testes) por ano para garantir o atendimento ao SIL requerido e levar em consideração que para testar o sistema, independente da configuração analisada, são necessárias quatro horas de parada da unidade, conforme apresentado, na seção 6.6.

Desta forma, a Tabela 6.8 e a Figura 6.10 apresentam o valor do OPEX para cada uma das alternativas propostas (ver Tabela 6.1) e para o seu cálculo foram considerados os valores apresentados nas Tabelas 6.2 e 6.5.

TABELA 6.8: OPEX (em US$/ano) por Alternativa Analisada

| Alternativas | Freqüência mínima paradas/ano | OPEX/ano (US$) |
|---|---|---|
| FIS A-1 | 15,783 | 1,262,634 |
| FIS B-1 | 15,235 | 1,218,825 |
| FIS C-1 | 1,783 | 142,617 |
| FIS D-1 | 0,619 | 49,498 |
| FIS E-1 | 0,624 | 49,929 |
| FIS A-2 | 5,707 | 456,538 |
| FIS B-2 | 4,998 | 399,827 |
| FIS C-2 | 1,471 | 117,647 |
| FIS D-2* | 0,200 | 16,000 |
| FIS E-2* | 0,200 | 16,000 |

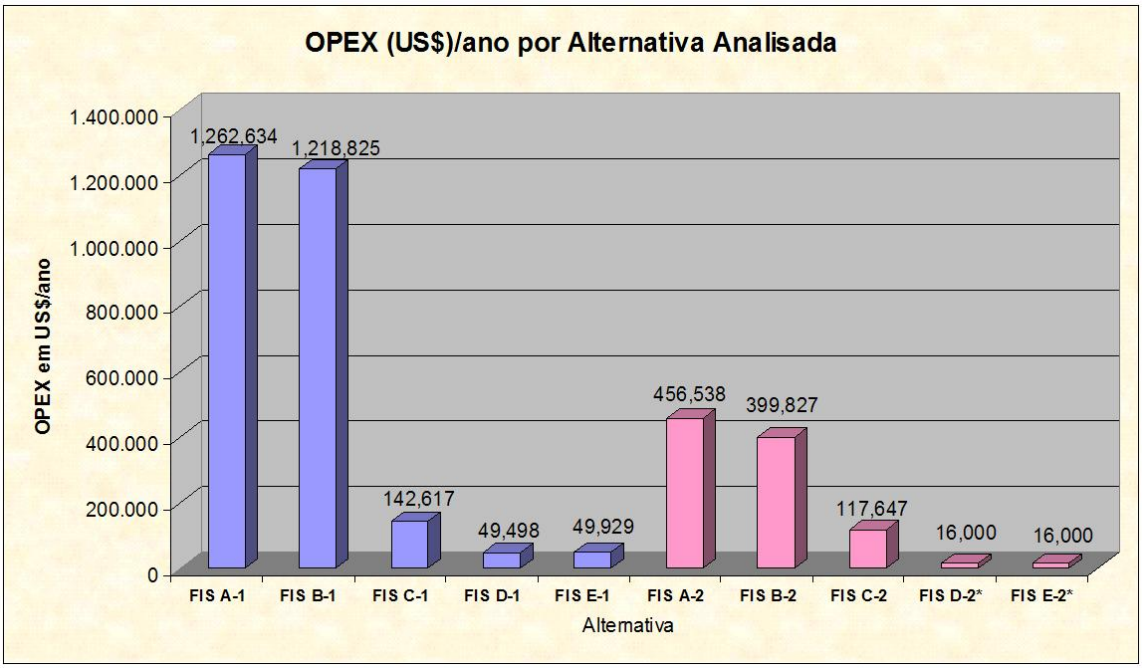


FIGURA 6.10: OPEX (em US$/ano) por Alternativa Analisada

Conforme discutido anteriormente, para o cálculo do OPEX é necessário determinar a freqüência esperada de paradas da planta necessária para testes/manutenção do SIS para garantir o atendimento a um nível de confiabilidade pré-determinado (SIL requerido). Desta forma, a Tabela 6.8, apresenta em sua segunda coluna, este número mínimo de paradas programadas do sistema para testes/manutenção de forma a garantir a operação da unidade, conforme o requisito de segurança pré-determinado. A seção 6.6 apresentou como premissa que o tempo necessário para a realização de testes na

FIS é de quatro horas, sendo uma hora para a realização do teste e três horas para trazer a planta de volta à operação normal. Foi dito ainda que a empresa incorre em uma "perda de produção" igual a US$20,000 (vinte mil dólares) por hora parada, de modo que cada teste acarreta uma perda total de US$80,000 (oitenta mil dólares). Desta forma, a terceira coluna da Tabela 6.8 apresenta o valor gasto por ano com paradas para testes da FIS de forma a garantir que a probabilidade de falha na demanda do sistema se mantenha no valor aceitável, ou seja, no limite máximo da faixa correspondente a SIL 3 ($\geq 10^{-4}$ e $< 10^{-3}$).

Pelos resultados apresentados na Tabela 6.8, é possível verificar que os custos anuais de operação para as alternativas FIS A-1 a FIS E-1 são, respectivamente, bem superiores aos valores apresentados para os custos anuais de operação das alternativas FIS A-2 a FIS E-2, respectivamente. Este resultado está justificado pelo fato das alternativas que envolvem a válvula de bloqueio tipo 1 demandarem um maior número de paradas para testes do sistema de segurança do que as alternativas que envolvem as válvulas de bloqueio tipo 2, conforme ilustrado na segunda coluna da referida tabela.

Em relação ao menor custo de operação anual, conforme esperado, dado a premissa apresentada na Tabela 6.6, as alternativas que apresentam o menor valor de custo anual de operação do sistema são as FIS D-2 e E-2. A alternativa que apresenta o maior custo de operação é a que requer o maior número de testes anuais, ou seja, a com maior probabilidade de falhar na demanda, neste caso, a FIS A-1, correspondente à configuração mais simples em termos de redundância, dentre as analisadas.

#### 6.7.2.3 Cálculo do RISKEX

Risco é usualmente definido de forma quantitativa como uma combinação matemática entre a freqüencia esperada de falha de um evento e as conseqüências da falha. No presente trabalho, as conseqüências do evento da falha são apresentadas em termos de custo. O conceito de "custo do risco" é um conceito estatístico. Uma despesa não ocorre realmente todo os anos, mas ocorre somente quando ocorre um evento (um acidente) (GOBLE 1998). O custo do evento individual pode ser extremamente alto. Todos trabalham para manter os custos destes eventos baixos. Se for feita a média do custo destes eventos em muitas instalações, por muitos anos, uma "média" do custo do risco por ano pode ser estabelecida. Se ações forem tomadas para reduzir a chance

de um evento, a média dos custos do risco serão também menores.

O terceiro e último fator que será considerado para o cálculo do custo do ciclo de vida das alternativas propostas para a função instrumentada de segurança do refervedor da unidade petroquímica, é o RISKEX (do inglês, *Risk Expenditures*), ou seja, o Custo do Risco. Cabe ressaltar que, para este fator, considerou-se apenas o custo das perdas relativas a falhas espúrias da FIS, já que os custos de acidentes decorrentes de falhas do SIS, seriam os mesmos, independentemente da alternativa analisada, pois todas têm necessariamente o mesmo valor de PFD correspondente o SIL 3, ou seja, todas as alternativas apresentam a mesma probabilidade de falhar na demanda, por premissa deste trabalho.

Falhas espúrias são falhas que levam a FIS a atuar conforme especificado sem que tenha ocorrido uma demanda do sistema, ou seja, o sistema de segurança atua bloqueando rapidamente a entrada de vapor (fonte de energia) para o refervedor R-01 da torre T-01, sem que tenha ocorrido alta pressão na mesma.

A freqüência esperada de desligamento espúrio reflete o número médio de vezes em que o sistema (SIS) falha por unidade de tempo (ou seja, o SIS atua sem que realmente tenha ocorrido uma demanda do mesmo). Este atributo é geralmente utilizado para avaliar os prejuízos econômicos que um dado tipo de falha causa durante um determinado período de tempo, o que, no presente trabalho, está relacionado a uma falha intrínseca do SIS que causa a sua atuação indevida para cada alternativa FIS analisada.

Diferentes configurações do sistema de segurança irão apresentar diferentes freqüências de desligamento espúrio, conforme dados apresentados na Tabela 6.9. Na seção 6.6, foi informado que este estudo adotou como premissa que cada parada da unidade, seja ela programada para a realização de um teste ou não, acarreta no mínimo três horas de parada, tempo este necessário para trazer a planta de volta à operação normal. Foi indicado ainda que por cada hora "parada", a empresa incorre em uma "perda de produção" igual a US$ 20,000, totalizando então uma quantia de US$ 60,000, cada vez que ocorre o acionamento do sistema de segurança.

Analisando a Tabela 6.9, observa-se que:

- a primeira coluna apresenta as alternativas analisadas;
- a segunda, a taxa de falha segura (ou espúria) de cada alternativa (por hora);

- a terceira coluna apresenta a freqüência esperada de paradas do sistema devido a falhas do sistema;

- a quarta coluna apresenta o custo referente ao retorno da unidade após uma falha espúria, levando em consideração o valor apresentado na coluna anterior e o valor de US$ 60,000 (sessenta mil dólares) por parada espúria da unidade.

- como cada componente possui sua própria freqüência de falha espúria (ver Tabela 6.2) e seu próprio tempo de reparo para o caso de uma falha espúria, o valor apresentado na quinta, sexta e sétimas colunas da Tabela 6.9, levam em consideração estes valores, bem como as configurações de cada uma das alternativas consideradas para a análise custo-beneficio proposta;

- a oitava e última coluna, apresenta o valor total do RISKEX por ano (em US$), que corresponde à soma dos valores apresentados nas colunas de número quatro a sete.

Cabe ressaltar que a freqüência de falha espúria de cada alternativa foi calculada levando em consideração as taxas de falhas espúrias de cada componente de cada uma das alternativas propostas (ver Tabela 6.2), bem como as respectivas arquiteturas. A freqüência esperada de paradas do sistema devido a falhas espúrias foi calculada multiplicando o valor da freqüência de falha espúria de cada alternativa (apresentada em horas) pelo número de horas em um ano (aproximadamente 8760 horas).

Tabela 6.9: RISKEX (US$/ano) por Alternativa Analisada

| Alternativa | Freqüência de falha espúria (/h) | Número de paradas/ano | Custo (3hs **) de Retorno da Unidade (US$) | Iniciador (US$) | Lógica (US$) | Atuador (US$) | RISKEXesp. /ano (US$) |
|---|---|---|---|---|---|---|---|
| FIS A-1 | 6,10E-06 | 5,34E-02 | 3,206,16 | 525,60 | 700,80 | 4,029,60 | 8,462,16 |
| FIS B-1 | 7,10E-06 | 6,22E-02 | 3,731,76 | 525,60 | 1,401,60 | 4,029,60 | 9,688,56 |
| FIS C-1 | 1,17E-05 | 1,02E-01 | 6,149,52 | 525,60 | 1,401,60 | 8,059,20 | 16,135,92 |
| FIS D-1 | 1,22E-05 | 1,07E-01 | 6,412,32 | 1,051,20 | 1,401,60 | 8,059,20 | 16,924,32 |
| FIS E-1 | 1,12E-05 | 9,83E-02 | 5,895,36 | 17,27 | 1,401,60 | 8,059,20 | 15,373,43 |
| FIS A-2 | 4,20E-06 | 3,68E-02 | 2,207,52 | 525,60 | 700,80 | 2,365,20 | 5,799,12 |
| FIS B-2 | 5,20E-06 | 4,56E-02 | 2,733,12 | 525,60 | 1,401,60 | 2,365,20 | 7,025,52 |
| FIS C-2 | 7,90E-06 | 6,92E-02 | 4,152,24 | 525,60 | 1,401,60 | 4,730,40 | 10,809,84 |
| FIS D-2* | 8,40E-06 | 7,36E-02 | 4,415,04 | 1,051,20 | 1,401,60 | 4,730,40 | 11,598,24 |
| FIS E-2* | 7,42E-06 | 6,50E-02 | 3,898,08 | 17,27 | 1,401,60 | 4,730,40 | 10,047,35 |

(**) Equivalente a US$ 60,000 (sessenta mil dólares)

A análise dos resultados apresentados na Tabela 6.9 e na Figura 6.11 indica que, em relação aos componentes da FIS, o atuador é o componente que mais contribui para o custo referente à perda de produção por paradas espúrias. Isto é facilmente justificado pelo fato das válvulas apresentarem maiores valores de taxa de falha espúria (ver Tabela 6.2). Outro ponto que cabe destacar é que, os valores do RISKEX espúrio (por ano) referentes às alternativas que estão relacionadas às válvulas do tipo 1, alternativas FIS A-1 a FIS E-1, apresentam maiores custos associados aos atuadores do que as alternativas relacionadas às válvulas do tipo 2, alternativas FIS A-2 a FIS E-2.

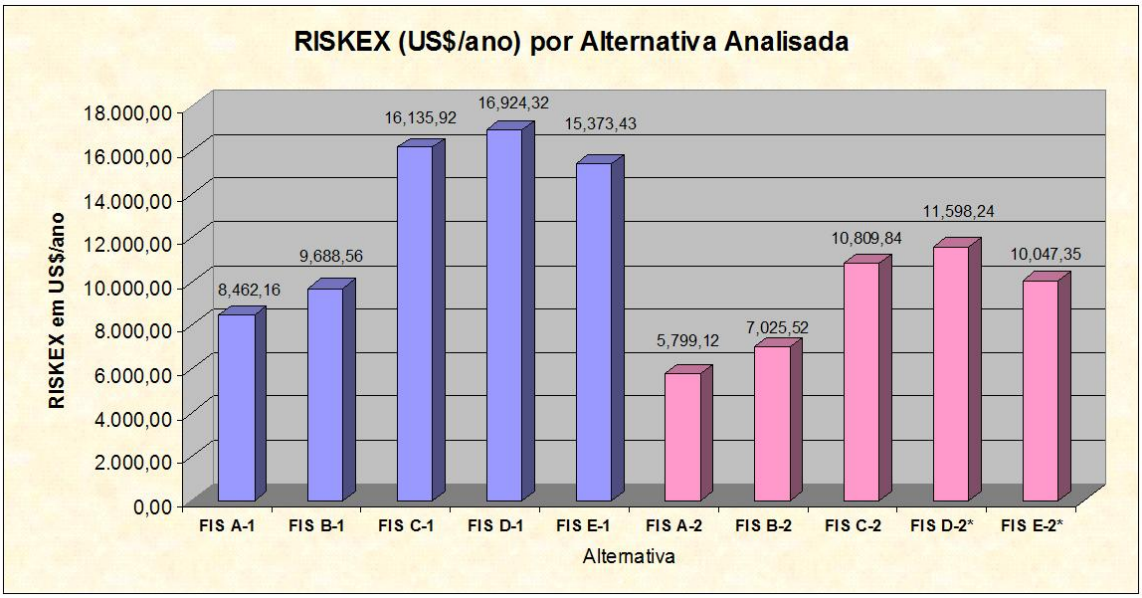


FIGURA 6.11: RISKEX (US$/ano) para as Alternativas Analisadas

Vale ressaltar também, o baixo custo associado à falha espúria do grupo de iniciadores (transmissores de pressão) nas alternativas correspondentes ao arranjo 2oo3, as alternativas FIS E-1 e FIS E-2. Este resultado é justificado pelo baixo valor da taxa de falha espúria para este tipo de arquitetura, que é da ordem de $10^{-8}$ para estes componentes.

De forma geral, o **maior** valor de RISKEX, levando em consideração todas as 10 alternativas analisadas, é a alternativa FIS D-1, alternativa correspondente à configuração: transmissor de pressão (1oo2), CLP (*hot standby*) e válvula tipo 1 (1oo2).

### 6.7.3 Análise Custo-Benefício

Conforme apresentado na seção 2.2, uma análise custo-benefício pode ser definida como uma avaliação comparativa dos custos e benefícios resultantes de maneiras alternativas para se atingir um determinado objetivo, como por exemplo, as possibilidades de implementação de diferentes configurações de um sistema de segurança para se atingir um nível de proteção requerido. Nesta seção, será apresentada a consolidação dos resultados apresentados nas seções anteriores, para cada uma das dez alternativas analisadas, com o intuito de avaliar a que apresenta a melhor a relação custo-benefício, tendo como parâmetro o custo do ciclo de vida (CCV) do sistema.

Conforme definido na equação 6.1, o CCV de cada alternativa proposta, pode ser entendido como correspondente à soma dos valores do CAPEX (ver Tabela 6.7), do OPEX (ver Tabela 6.8) e do RISKEX (ver Tabela 6.9). Para fins de avaliação do CCV, os custos do OPEX, do RISKEX e os custos totais de cada configuração são expressos na Tabela 6.10, na forma de Valor Presente Líquido - VPL (O CAPEX já é expresso em VPL). Para tanto, leva-se em consideração o período de vida útil e uma taxa de juros, que reflete o custo de capital de mercado.

Conforme CASAROTTO FILHO (2000), para o cálculo do valor presente líquido (VPL) do OPEX e do RISKEX, foi utilizada a equação 6.3, onde "A" representa o valor anual, "i" a taxa de juros (assumido como 12% ao ano neste trabalho) e, "n" o período de vida útil da instalação, considerado como 30 anos (valor típico da indústria de processos).

$$P = A\frac{(1+i)^n - 1}{i(1+i)^n} \tag{6.3}$$

onde:

**P** = valor presente (dólares);

**A** = valor anualizado (dólares/ano);

**i** = taxa de juros anual; e

**n** = período de tempo em anos (normalmente o tempo esperado de vida útil da instalação).

A Tabela 6.10, sumariza os resultados para cada uma das dez alternativas analisadas, no que tange o cálculo do custo do ciclo de vida. A primeira coluna da referida tabela apresenta a alternativa que está sendo considerada; a segunda, o CAPEX; a terceira, OPEX, representa o OPEX expresso em valor presente líquido, a quarta, o RISKEXesp, representa o RISKEX também expresso em valor presente líquido, e finalmente, a quinta coluna apresenta o custo do ciclo de vida para a unidade, em VPL, considerando o CAPEX, o OPEX e o RISKEX.

Tabela 6.10: Custo do Ciclo de Vida por Alternativa Analisada

| Alternativa | CAPEX (US$) | OPEX (US$) em VPL | RISKEXesp (US$) em VPL | Custo do Ciclo de Vida (US$) em VPL |
|---|---|---|---|---|
| FIS A-1 | 41,000 | 10,170,753 | 68,164 | 10,279,917 |
| FIS B-1 | 56,000 | 9,817,860 | 78,043 | 9,951,903 |
| FIS C-1 | 71,000 | 1,148,804 | 129,978 | 1,349,782 |
| FIS D-1 | 72,000 | 398,712 | 136,329 | 607,041 |
| FIS E-1 | 73,000 | 402,184 | 123,836 | 599,020 |
| FIS A-2 | 46,000 | 3,677,500 | 46,713 | 3,770,213 |
| FIS B-2 | 61,000 | 3,220,676 | 56,592 | 3,338,268 |
| FIS C-2 | 81,000 | 947,667 | 87,075 | 1,115,742 |
| FIS D-2* | 82,000 | 89,116 | 93,426 | 304,309 |
| FIS E-2* | 83,000 | 104,531 | 80,933 | 292,816 |

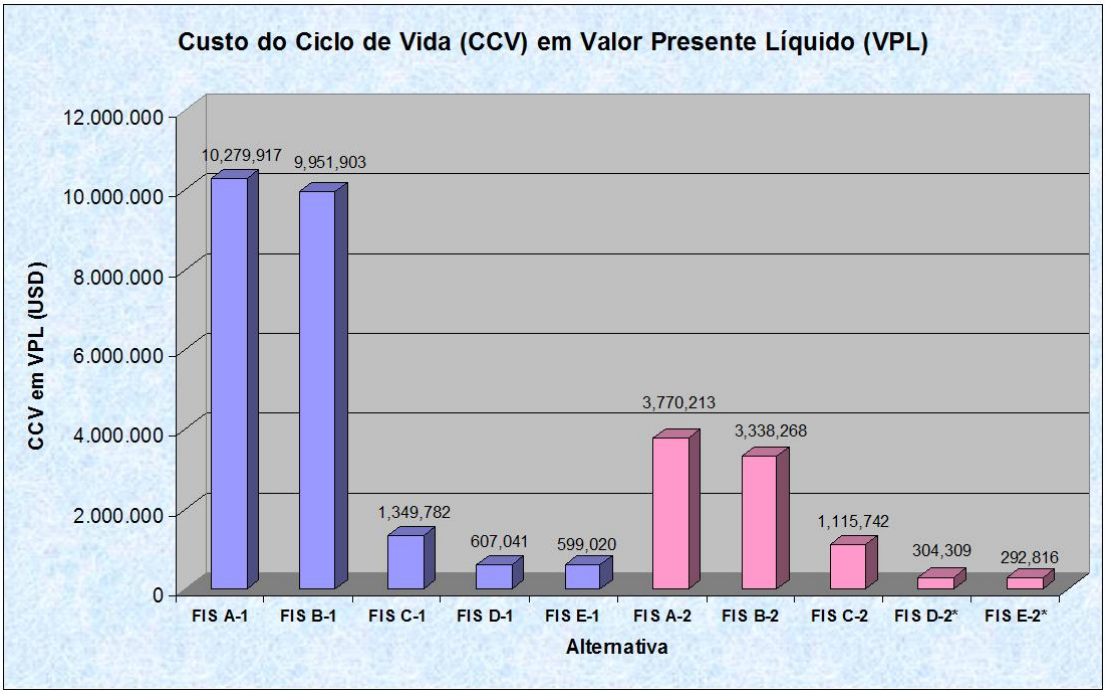


Figura 6.12: Gráfico do Custo do Ciclo de Vida e Alternativas

Pelos resultados apresentados na Tabela 6.10 e visualizados na Figura 7.2, é possível verificar que a alternativa que apresenta o menor valor de custo do ciclo de vida, considerando tanto os custos para investimentos quanto para a operação do sistema de forma a atender o SIL 3 requerido e custos referentes a falhas espúrias, é a alternativa **FIS E-2***. Em seguida, vem a alternativa **FIS D-2***. Estas alternativas consideram redundância em todos os elementos da FIS e apresentam respectivamente a seguinte arquitetura: transmissor de pressão (2oo3), CLP (*hot standby*) e válvula de bloqueio tipo 2 (1oo2), com a realização de testes parciais do atuador a cada 15 dias; e transmissor de pressão (1oo2), CLP (*hot standby*) e válvula de bloqueio tipo 2 (1oo2) com a realização de testes parciais do atuador a cada 15 dias.

Cabe ressaltar que o CCV das alternativas FIS D-2 e FIS E-2 foram calculados com o intervalo entre testes igual a 5 anos, devido à limitação natural, imposta pela política de manutenção geral da planta (a cada 5 anos). Os valores do CCV destas alternativas seriam ainda menores se tivessem sido calculadas com os tempos máximos do intervalo de teste com que ainda conseguiriam satisfazer a SIL 3, que foram de aproxidamente 6 e 7 anos, respectivamente.

É possível ainda verificar por estes resultados, que a parcela de maior impacto no custo do ciclo de vida para a maioria das alternativas é o valor do OPEX, ou seja, o custo relativo ao número de paradas necessárias para testar o sistema e manter assim o nível de SIL 3 requerido, inclusive para a alternativa com o menor valor do CCV, a **FIS E-2***. Portanto, pode-se dizer que, para o caso em questão, é extremamente vantajoso o investimento na aquisição de uma configuração do sistema mais redundante e sofisticada (por exemplo, com capacidade para a realização de testes parciais) em comparação com as configurações mais simples.

No que tange o CAPEX, algumas vantagens alcançadas com investimentos em confiabilidade e segurança de sistemas/instalações são relacionadas a seguir (ERIKSEN & SAUCIER 2000):

- Redução de gastos e custos pode ser alcançada evitando atenção para áreas que não são críticas, aperfeiçoando áreas onde a relação custo/benefício é maior. Por exemplo, considerações de disponibilidade podem ser usadas para justificar o investimento no aumento de uma redundância funcional como também a aquisição

de um dado equipamento com uma maior confiabilidade.

- Considerações de confiabilidade e de disponibilidade podem levar à descoberta de excelentes oportunidades para a proposição de melhorias durante as fases conceituais e de projeto evitando assim alterações em projetos já consolidados onde o custo de mudança é muito maior. Além disso, quanto mais tarde forem implementadas as melhorias nos projetos, isto é, em projetos mais avançados ou consolidados, maiores serão as chances de perdas de receitas e de gastos excessivos, desnecessários, que impedem oportunidades de melhorias das receitas operacionais.

Os pontos destacados acima tornam-se bastante evidentes ao se comparar os resultados obtidos com as alternativas FIS B-1 e FIS C-1. A diferença entre estas duas alternativas é apenas na redundância alocada ao atuador (válvula de bloqueio tipo 1). A simples alteração de uma configuração com uma válvula, para outra com duas válvulas num arranjo 1oo2, impacta significativamente no resultado do custo do ciclo de vida, chegando a resultar numa diferença de um fator de até 7 vezes maior, por exemplo, o CCV da alternativa FIS C-1 equivale a aproximadamente 13,5% do valor do CCV da alternativa FIS D-1. Cabe destacar que o mesmo raciocínio é válido para a análise das alternativas FIS B-2 e FIS C-2.

É importante destacar que, além das premissas e dados apresentados na seção 6.6, outros pontos têm que ser destacados, de forma a ratificar os resultados apresentados acima: (1) não foram considerados custos de acidentes como uma parcela do RISKEX, já que o custo do acidente seria o mesmo independente da alternativa analisada, (2) não foi descontado do custo do ciclo de vida de cada alternativa o custo para se testar o sistema quando o teste ocorre durante a parada programada da unidade (a cada 5 anos) e (3) considerou-se que as alternativas FIS D-2 e FIS E-2 serão testadas no máximo a cada 5 anos, durante a parada programada para manutenção da unidade, embora apresentem um valor de PFD baixo o suficiente para permitir intervalos maiores de testes totais do sistema.

#### 6.7.3.1 Análise Custo-Benefício - Considerando as Restrições de Arquitetura da Norma IEC 61508

Conforme discutido na seção 3.7, uma vez obtidos os resultados das PFDs de cada componente da malha de segurança, estes devem ser combinados de forma a verificar se o SIL da malha de segurança atende ao SIL requerido pela função de segurança. No entanto, para que esta verificação esteja de acordo com a Norma IEC 61508, devem-se também considerar as restrições impostas pela norma quanto ao máximo nível de integridade (SIL) atingível por uma malha de segurança em função das características dos seus componentes.

As restrições de arquitetura de integridade de segurança de *hardware* são dados em termos de três parâmetros (OLF 2004):

- A tolerância à falha de *hardware* do subsistema (ou do inglês, *Hardware Fault Tolerance* - HFT);
- A fração de falhas seguras (ou do inglês, *Safe Failure Fraction* - SFF); isto é, a fração de falhas que podem ser consideradas "seguras" por serem detectadas por testes de diagnósticos ou porque não causam perda da função de segurança;
- Tipo do componente, ou seja, "Tipo A" ou "Tipo B" (ver seção 3.7).

Desta forma, as restrições de arquitetura devem ser levadas em consideração para a determinação do nível de integridade de segurança máximo que pode ser assumido por uma função de segurança. Conforme pode ser verificado pelas tabelas 3.3 e 3.4, o maior valor de SIL que pode ser assumido para uma função de segurança é limitado pela Tolerância à Falha de *Hardware* (HFT) e pela Fração de Falha Segura (SFF) dos subsistemas que desempenham aquela função de segurança.

Dado este cenário, esta seção tem por objetivo analisar as alternativas e os resultados apresentados nas seções anteriores sob o enfoque das restrições de arquitetura da Norma IEC 61508, visando verificar a sua influência na análise custo-benefício, enfoque deste trabalho.

A seção anterior apresentou como resultado, que a alternativa "**FIS E-2***" é a que apresenta a melhor a relação custo-benefício, tendo em vista o valor do custo do ciclo

de vida do sistema. Desta forma, esta será a alternativa avaliada quanto às restrições de arquitetura citadas.

A Tabela 6.11, apresenta a análise para a alternativa selecionada, levando em consideração, as Tabelas 3.3 e 3.4, que apresentam a combinação dos parâmetros pertinentes (HFT, SFF e Tipo do Componente) e os resultados do maior nível de SIL que pode ser atingível por uma malha de segurança em função das características de seus componentes. Cabe destacar que o parâmetro SFF foi calculado conforme apresentado pela equação 3.1.

TABELA 6.11: Restrições de Arquitetura - Análise Custo Benefício

| Alternativa | Componentes | Tipo | HFT | SFF | Máximo SIL |
|---|---|---|---|---|---|
| FIS E-2* | Transmissor de Pressão (2oo3) | B | 2 | 0,75 | SIL 3 |
| | CLP hot standby (1oo2) | B | 1 | 0,95 | SIL 3 |
| | Válvula de Bloqueio Tipo 2* (1oo2) | B | 1 | 0,62 | SIL 2 |
| | | | | | SIL 2 |

Pelo resultado apresentado na Tabela 6.11, é possível verificar que, embora individualmente, o grupo de iniciadores e da lógica possa atender a um requisito de SIL 3, levando em consideração as restrições de arquitetura apresentadas, o grupo das válvulas atende no máximo ao SIL 2, fazendo com que a arquitetura proposta para a FIS, atenda apenas ao SIL 2 e não ao SIL 3 conforme requerido. No entanto, cabe ressaltar, que considerou-se que os equipamentos são do Tipo B e este é um ponto um pouco delicado em relação à sua definição. Analisando as Tabelas 3.3 e 3.4, e tendo os resultados da HFT e da SFF apresentados na Tabela 6.11, é possível verificar que o grupo limitante é o das válvulas, pois, a não ser que elas sejam consideradas do Tipo A, não é possível atingir o SIL 3 com esta alternativa selecionada. Este assunto voltará a ser discutido mais adiante neste capítulo.

Dado que a alternativa "FIS E-2*" não atende aos requisitos de arquitetura propostos pela Norma IEC 61508, todas as outras nove alternativas serão analisadas com o intuito de verificar se alguma delas atende o SIL 3, utilizando estes critérios. A Tabela 6.12 mostra as premissas consideradas neste trabalho para cada componente com relação ao seu tipo. A Tabela 6.13, apresenta os resultados (SIL máximo permitido) para cada alternativa proposta.

Tabela 6.12: Componentes identificados pelo Tipo

| Componente | Tipo |
|---|---|
| Transmissor de Pressão | B |
| CLP | A |
| CLP *hot standby* | B |
| Válvula de bloqueio Tipo 1 | A |
| Válvula de bloqueio Tipo 2 | B |

Tabela 6.13: Resultado das Alternativas Propostas

| Alternativa | Máximo SIL |
|---|---|
| FIS A-1 | SIL 1 |
| FIS B-1 | SIL 1 |
| FIS C-1 | SIL 1 |
| FIS D-1 | SIL 2 |
| FIS E-1 | SIL 3 |
| FIS A-2 | SIL 1 |
| FIS B-2 | SIL 1 |
| FIS C-2 | SIL 1 |
| FIS D-2* | SIL 2 |

Analisando os resultados apresentados na Tabela 6.13, fica claro ser a alternativa **FIS E-1** a única que atende às restrições de segurança discutidas nesta seção. No entanto, cabe destacar que, conforme pode ser verificado na Tabela 6.10, o custo do ciclo de vida para esta alternativa, em valor presente líquido, é de US$ 599,020 (quinhentos e noventa e nove mil e vinte dólares), um valor aproximadamente **duas vezes maior** do que o resultado apresentado pela alternativa **FIS E-2***, sem a consideração das restrições de arquitetura.

Desta forma, deste ponto da análise em diante, cabem duas alternativas ao analista que tomará a decisão quanto à alternativa que será proposta para o sistema de bloqueio do refervedor: indicar a alternativa **FIS E-1** como a que apresenta a melhor relação custo-benefício e atende aos requisitos de restrição de arquitetura da Norma IEC 61508, ou propor uma nova configuração para a alternativa **FIS E-2*** que atenda aos requisitos de arquitetura da norma e comparar a sua relação custo-benefício com a anteriormente selecionada.

De forma a realmente verificar se a alternativa **FIS E-1** é a que deve ser recomendada para o sistema, proporemos uma nova alternativa, deste ponto em diante, denomi-

nada **FIS E-2****. Analisando a Tabela 3.4 é possível verificar que de forma a conseguir um valor máximo de SIL 3 para o grupo de válvulas, o que garantiria o atendimento à restrição SIL 3 para a FIS, as alternativas possíveis são: um maior valor de HFT ou um maior valor de SFF. A configuração proposta visa testar o novo valor do custo do ciclo de vida para a alternativa **FIS E-2****, através de um **maior valor de HFT** para este grupo de válvulas. Desta forma, a configuração proposta consiste em se adicionar mais uma válvula de bloqueio, formando assim uma lógica 1oo3 para os atuadores. A única alteração em relação à configuração anterior é o diferente arranjo do grupo de válvulas de 1oo2 para 1oo3, o que permite à nova configuração satisfazer um máximo SIL igual a 3.

Realizando os cálculos discutidos e apresentados na seção 6.7 para a alternativa **FIS E-2****, temos os resultados apresentados na Tabela 6.14:

Tabela 6.14: OPEX para a Alternativa FIS E-2

| Alternativa | Número mínimo paradas/ano | OPEX/ano (US$) |
|---|---|---|
| FIS E-2** | 0,200 | 16,000 |

Cabe destacar que, para a avaliação desta alternativa, foi adotada a mesma premissa de que a FIS será testada a cada, pelo menos 5 anos, durante a parada programada da unidade, embora deva ficar claro que o sistema poderia ser testado em um intervalo de tempo maior do que este para o atendimento ao requisito SIL 3, dado que a configuração 1oo3 para o grupo das válvulas possui ainda uma menor probabilidade de falhar na demanda do que os arranjos anteriores para os quais foi adotada esta premissa.

Tabela 6.15: RISKEX para a Alternativa FIS E-2

| Alternativa | $\lambda_S$ (/h) | Custo * (US$) | I (US$) | L (US$) | A (US$) | RISKEXesp. /ano (US$) |
|---|---|---|---|---|---|---|
| FIS E-2** | 1,01E-05 | 5,317, 20 | 17,27 | 1,401,60 | 7,095,60 | 13,831,67 |

(*) Equivalente a 3h para retorno da unidade à operação, US$ 60,000 (sessenta mil dólares)
Nota 1: $\lambda_S$ igual a 1,01E-05 corresponde a um número de paradas/ano igual a 8,86E-02.

Desta forma, o valor do custo do ciclo de vida para a nova alternativa é dado pela Tabela 6.16, onde é possível verificar também os valores do OPEX e do RISKEX, expressas em valor presente líquido (VPL).

Tabela 6.16: Resultado do CCV para a Alternativa FIS E-2

| Alternativa | CAPEX (US$) | OPEX (US$) em VPL | RISKEXesp (US$) em VPL | Custo do Ciclo de Vida (US$) em VPL |
|---|---|---|---|---|
| FIS E-2** | 103,000 | 128,883 | 111,417 | 343,300 |

De forma a facilitar a conclusão do estudo comparativo entre as alternativas FIS E-1, FIS E-2* e FIS E-2**, a Tabela 6.17 e a Figura 6.13 apresentam novamente os resultados finais para cada uma destas opções.

Tabela 6.17: Resultado Final do CCV para as Alternativas Selecionadas

| Alternativa | CAPEX (US$) | OPEX (US$) em VPL | RISKEXesp (US$) em VPL | Custo do Ciclo de Vida (US$) em VPL |
|---|---|---|---|---|
| FIS E-1 | 73,000 | 402,184 | 123,836 | 599,020 |
| FIS E-2* | 83,000 | 128,883 | 80,933 | 292,816 |
| FIS E-2** | 103,000 | 128,883 | 111,417 | 343,300 |

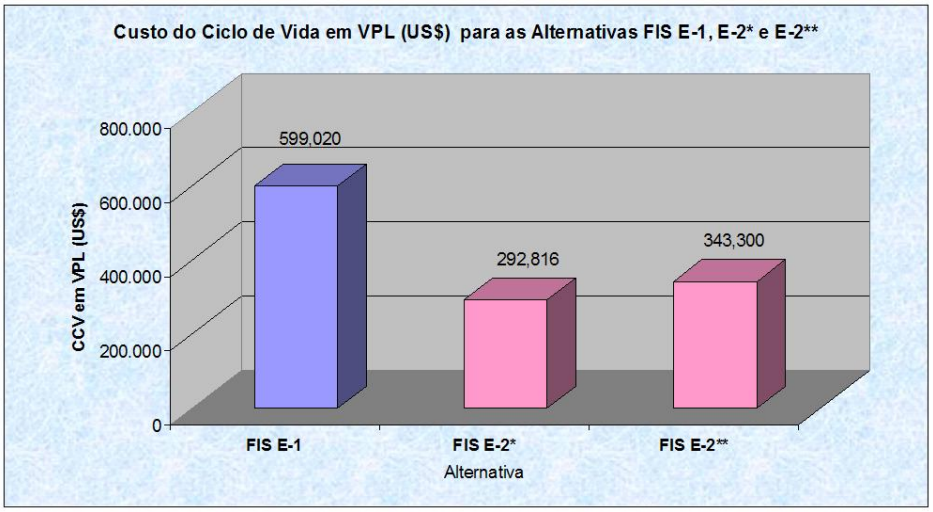


Figura 6.13: Custo do Ciclo de Vida em VPL (US$) para as Alternativas FIS E-1, E-2* e E-2**

Pelos resultados apresentados na Tabela 6.17, é possível verificar que a alternativa **FIS E-2**** ainda é mais vantajosa do que a alternativa **FIS E-1**, ou seja, a

proposição de uma nova alternativa, onde, de forma a atender às restrições de arquitetura de *hardware* da Norma IEC 61508, altera-se a configuração do grupo dos atuadores (válvula de bloqueio tipo 2) de forma a conseguir um valor de HFT maior, de HFT igual a 1 (arranjo 1oo2) para HFT igual a 2 (arranjo 1oo3) se mostrou bem sucedida.

O valor do CCV da alternativa **FIS E-2***(a alternativa que apresenta o menor valor do CCV, mas não atende às restrições de arquitetura) apresenta uma diferença em relação a alternativa **FIS E-2**** (que atende aos requisitos de restrição de arquitetura) de US$ 50,102 (cinqüenta mil cento e dois dólares), enquanto que para a alternativa **FIS E-1**, apresenta uma diferença de US$ 255,565 (duzentos e cinqüenta e cinco mil quinhentos e sessenta e cinco dólares), ou seja, um valor cerca de cinco vezes maior. Desta forma, a alternativa **FIS E-2**** é a melhor opção, caso a organização vise atender à Norma IEC 61508 e dadas as premissas consideradas nesta análise.

## 6.8 Análise de Sensibilidade e Comentários Finais

A análise custo-benefício, utilizando como ferramenta uma análise do custo do ciclo de vida de diferentes alternativas de um sistema de segurança, estudo de caso proposto para este trabalho (identificação da melhor configuração de um sistema de segurança de modo que o mesmo atenda a um requisito SIL 3) apresentado na seção 6.7, resultou na apresentação de duas alternativas, conforme destacado a seguir:

- Alternativa **FIS E-2*** (caso não seja obrigatório o atendimento às restrições de arquitetura da Norma IEC 61508);
- Alternativa **FIS E-2**** (caso seja obrigatório o atendimento às restrições de arquitetura da Norma IEC 61508).

Assumindo que o atendimento à Norma não é obrigatório no Brasil e que a Norma é apenas utilizada como referência para a avaliação da PFD de cada alternativa, a análise de sensibilidade será realizada considerando a alternativa **FIS E-2***. Então, de forma a verificar a robustez e a consistência dos resultados em relação à alguns parâmetros críticos, esta seção objetiva apresentar uma sucinta análise de sensibilidade, através da análise do impacto de variações desses parâmetros sobre os resultados dos

cálculos realizados na seção 6.7. Esta análise de sensibilidade será realizada para três parâmetros: o coeficiente de diagnóstico de teste parcial, o custo das válvulas e o intervalo entre testes parciais.

Em relação ao coeficiente de diagnóstico de teste parcial, conforme cita a seção 6.6, considerou-se um coeficiente igual a 0,8 para $\lambda_D$, ou seja, 80% das falhas detectadas são testadas durante a realização de um teste parcial neste componente. Realizada uma análise de sensibilidade do resultado em relação a este parâmetro, foi possível verificar que, para até um valor de coeficiente igual a 0,69 ou 69%, o sistema ainda atende ao requisito de SIL 3, para um intervalo entre testes de 5 anos. A Figura 6.14 apresenta a variação do valor da PFD da FIS analisada em relação à variação do coeficiente de diagnóstico de teste parcial.

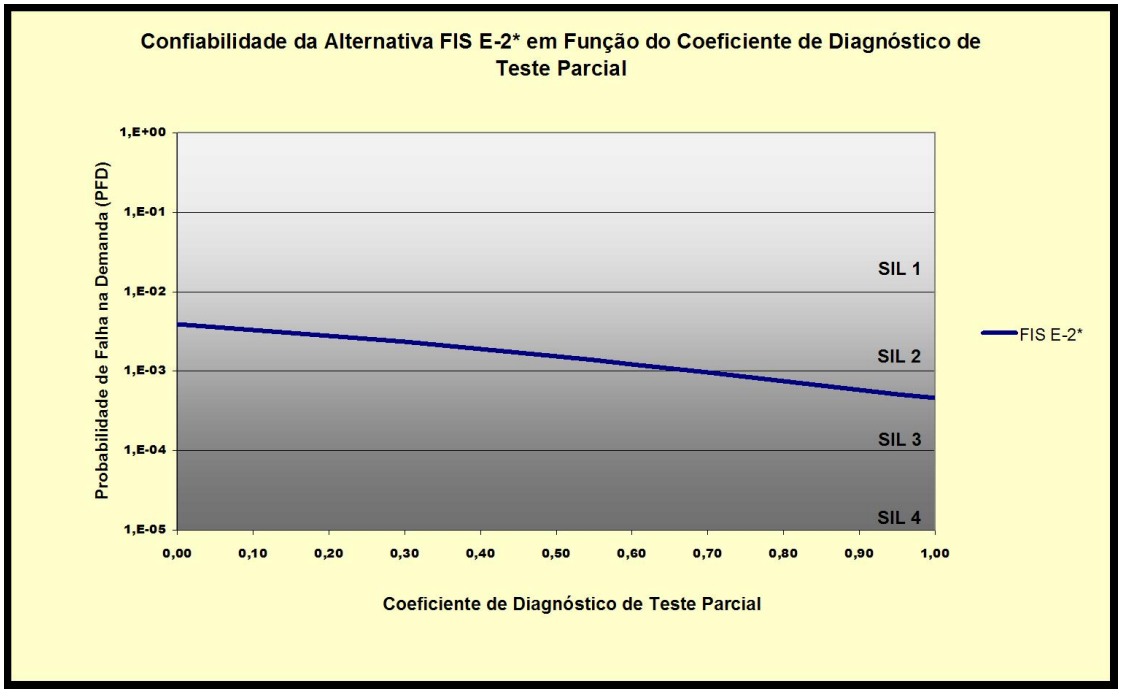


FIGURA 6.14: Confiabilidade da Alternativa FIS E-2* em Função do Coeficiente de Diagnóstico de Teste Parcial

Em relação ao custo da válvula do tipo 2 (com posicionador, que permite a realização de testes parciais), adotou-se como dado do estudo que seu custo é cerca de 25% maior do que o da válvula do tipo 1 (com solenóide), conforme apresenta a Tabela 6.2. Realizada uma análise de sensibilidade do resultado em relação a este parâmetro, foi possível verificar que mesmo que o valor da válvula do tipo 2 seja duas vezes maior do que o valor da válvula tipo 2, ou seja, um valor de US$ 30,000 (trinta mil dólares),

ainda assim, a alternativa FIS E-2* continua sendo a mais custo eficiente dentre as analisadas. A Figura 6.15 apresenta a variação do valor do CCV da FIS analisada em relação à variação do valor da válvula tipo 2.

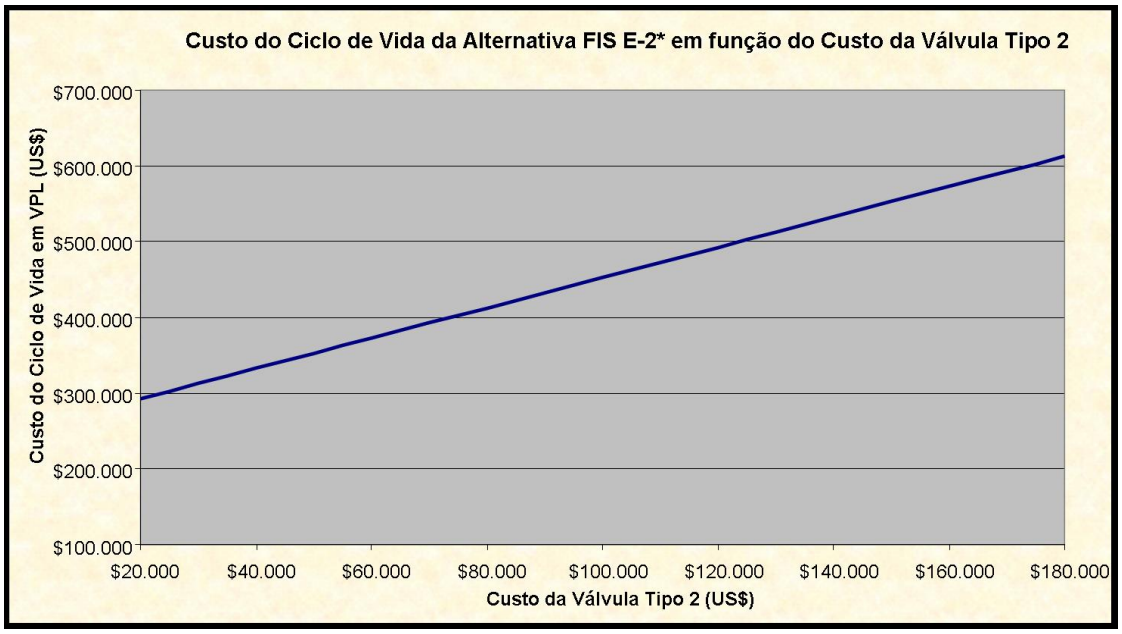


FIGURA 6.15: Custo do Ciclo de Vida em VPL (US$) da FIS E-2* em Função do Custo da Válvula Tipo 2 (US$)

Em relação ao intervalo entre testes parciais, conforme cita a seção 6.6, considerou-se uma periodicidade de 15 dias (360 horas). Realizada uma análise de sensibilidade do resultado em relação a este parâmetro, foi possível observar que, considerando um intervalo de testes parcias de até aproximadamente 9 meses (6645 horas), e considerando um teste total do sistema a cada 5 anos, durante a parada programada da unidade, o sistema ainda atende ao SIL 3 requerido, sem que sejam necessários testes parciais a cada 15 dias dos atuadores. A Figura 6.16 apresenta a variação do valor da PFD da FIS analisada em relação à variação do intervalo de testes parciais.

Cabe destacar que como não foram considerados custos para a realização de testes parciais, dado que assumiu-se que estes custos são muito pequenos, pois envolvem somente custo de mão de obra, são feitos rapidamente e não envolvem perda de produção, o custo do ciclo de vida não é afetado por esta variação no intervalo de testes parciais do sistema.

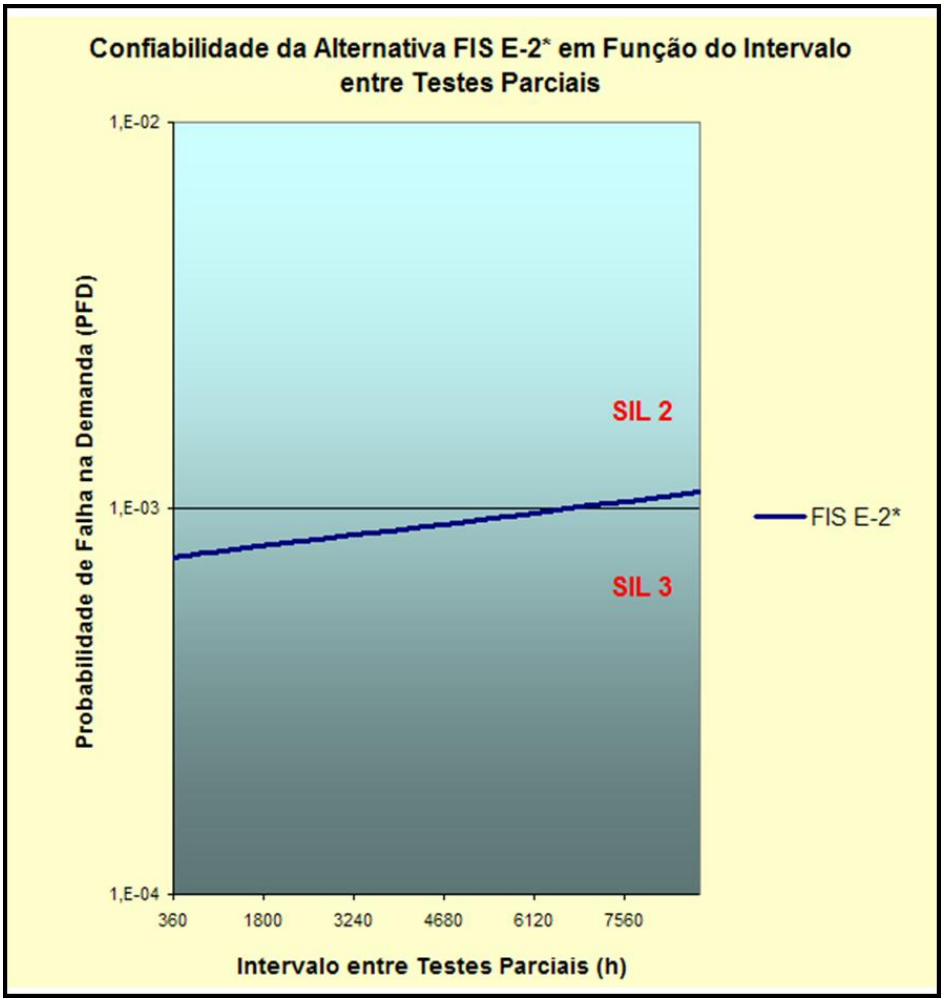


FIGURA 6.16: Confiabilidade da Alternativa FIS E-2* em função do intervalo entre Testes Parciais

Em função dos dados apresentados acima, é possíver verificar a consistência do resultado em relação à alternativa selecionada como a que apresenta a melhor relação custo-benefício, ou o menor custo do ciclo de vida, de todas as alternativas propostas para a análise do sistema de segurança de bloqueio de um refervedor (um sistema HIPPS), descrito na seção 6.3.

# Capítulo 7

# Conclusões e Proposta para Trabalhos Futuros

Para a operação segura de uma unidade industrial é fundamental que sejam implementados mecanismos para a redução de riscos a níveis toleráveis. A redução dos riscos pode ser obtida por um projeto físico adequado, por estratégias de controle do processo ou por instrumentação dedicada a implementar funções de segurança que minimizem a ocorrência de situações de risco. A instrumentação dedicada exclusivamente à segurança constitui o chamado "Sistema Instrumentado de Segurança (SIS)" e a avaliação da sua eficácia é fundamental para a garantia de uma operação segura, ou seja, dentro de níveis de risco considerados aceitáveis.

A efetividade do SIS é medida através da sua "Probabilidade de Falha na Demanda - PFD" ou do seu correspondente "Fator de Redução de Risco - FRR", e é classificada através de um índice chamado "Nível de Integridade de Segurança" (em inglês, *Safety Integrity Level* - SIL).

Ao fornecerem os métodos de análise de risco e o nível de SIL Requerido para uma determinada função de segurança com base no risco que ela se destina a proteger, as normas resolveram um dos problemas que mais perturbavam a cabeça dos projetistas de sistemas de proteção: "Que nível especificar para a confiabilidade do sistema de proteção?". Esta pergunta tem reflexos diretos sobre o nível de redundância das partes do sistema, sobre as políticas de teste e manutenção do sistema e sobre a política operacional da instalação em caso de falhas detectadas no sistema de proteção. São,

portanto, questões de largo alcance e que podem ter conseqüências significativas, tanto sobre a segurança quanto sobre a eficiência produtiva (disponibilidade) das instalações de processos. Na realidade, pode-se dizer que as normas resolveram de forma prática a questão dos critérios de 'tolerabilidade de riscos', pelo menos no que concerne à especificação de Sistemas Instrumentados de Segurança.

O objetivo da otimização de um determinado sistema é maximizar ganho (ou desempenho) com a operação do referido sistema, e o desenvolvimento de métodos de otimização que abordam de maneira integrada o maior número possível de parâmetros relacionados a este desempenho merece destaque, principalmente quando são considerados conjuntamente desempenho e segurança.

O aumento da confiabilidade geralmente implicará num aumento de custo, mas o fato de se conseguir atingir um alto nível de confiabilidade poderá proporcionar uma grande economia futura em termos de maior eficiência produtiva e evitar a perda de vidas humanas. Dado este cenário, existe a necessidade de se preservar um balanço econômico entre o custo da confiabilidade e as vantagens decorrentes da implementação de um alto nível de confiabilidade. Assim, para qualquer objeto funcional não é de interesse saber apenas se o mesmo é funcional, mas sim **quão confiável ele é**, ou seja, se ele é **suficientemente confiável**. A introdução da palavra "suficientemente" implica numa quantificação do conceito de confiabilidade. Em outras palavras, para se usar qualquer tipo de balanço econômico, a confiabilidade deve ser definida e usada de modo a se constituir numa quantidade mensurável.

A utilização de técnicas de análise de confiabilidade permite que os níveis de confiabilidade de várias configurações alternativas para o projeto de um determinado sistema de proteção sejam avaliados quantitativamente. Sem dúvida, os índices quantitativos obtidos na análise constituem-se em elementos importantes para o projetista, possibilitando o conhecimento das variações relativas à confiabilidade entre as diferentes configurações e para a identificação dos componentes do sistema que mais contribuiem para a sua probabilidade de falha. No entanto, na grande maioria das vezes, a variação relativa dos índices de confiabilidade não se constitui em argumento suficiente para a tomada de decisão relativa à escolha de uma das alternativas consideradas. Portanto, de um modo geral, o processo de tomada de decisão requer a realização de um balanço entre os custos de cada configuração e os seus benefícios associados. A realização deste

balanço é o fundamento básico de uma Análise Custo-Benefício.

Em se tratando de sistemas de segurança, os benefícios estão relacionados à redução do número de acidentes na instalação, com conseqüente redução do nível de perdas esperadas, em virtude da utilização de configurações com maior nível de confiabilidade. A composição das perdas esperadas pode envolver tanto a perda de vidas humanas como as perdas econômicas, sendo estas últimas compostas pelas perdas de instalações (custos de reposição ou de reparo de equipamentos) e perdas relativas à interrupção da produção. Outro aspecto importante a ser considerado no caso de sistemas de segurança, refere-se ao custo associado à ocorrência de desligamentos indevidos da instalação causados por falhas espúrias do sistema de segurança. Este custo está diretamente vinculado à estrutura lógica de cada alternativa estudada. Assim sendo, a mudança de uma configuração para outra, pode levar a um aumento ou uma diminuição do número de desligamentos indevidos, resultando em um benefício ("ganho") ou em um custo ("perda") econômica.

## 7.1 Conclusões e Comentários Finais

Neste trabalho foi proposta a aplicação de técnicas de análise de confiabilidade e de análise do custo do ciclo de vida, com o objetivo integrado de tomada de decisão na escolha de uma alternativa que apresentasse a melhor a relação custo-benefício para um determinado sistema de segurança de uma empresa do ramo petroquímico, de forma que tal sistema atendesse a um determinado requisito de confiabilidade mínimo pré-estabelecido.

O modelo desenvolvido permite a proposição e comparação de várias alternativas de configuração para a FIS, além de fornecer subsídios para a formulação da estratégia de implementação a ser adotada pelos responsáveis pelo projeto do sistema de segurança proposto. Foi utilizada a modelagem do custo do ciclo de vida como abordagem econômica, por ser uma modelagem importante do ponto de vista do usuário que lida com a operacionalidade do seu projeto ao longo da sua vida útil.

Foram propostas inicialmente dez alternativas para a configuração do sistema de segurança do estudo de caso apresentado. Conforme citado, todas estas alternativas apresentam como premissa um requisito mínimo de confiabilidade (SIL 3 ou PFD entre

$1,0 \times 10^{-4}$ e $1,0 \times 10^{-3}$) a ser atingido. Desta forma, a primeira avaliação realizada foi a determinação das condições sob as quais cada uma destas alternativas atende a este nível requerido de confiabilidade. Para verificar se o SIL atingido é compatível com o que foi desejado, há inúmeras técnicas. Neste trabalho foi utilizado o método do diagrama de blocos e as equações analíticas fornecidas no Apêndice B da Parte 6 da Norma IEC 61508 ((IEC-61508 1998)) para a avaliação da PFD do sistema de segurança analisado. Cabe ressaltar que este apêndice apresenta apenas as equações para o cálculo da PFD de arquiteturas 1oo1, 1oo2, 1oo2D, 2oo2 e 2oo3.

Dado a adequação de todas as alternativas propostas ao nível de confiabilidade requerido, este trabalho utilizou a modelagem do custo do ciclo de vida, considerando o CAPEX (custo de aquisição dos equipamentos), o OPEX (custo necessário para operação do sistema) e o RISKEX (custo associado a paradas de produção causadas por falhas espúrias) para a avaliação custo-benefício das alternativas analisadas. Os resultados obtidos no estudo de caso permitem constatar o potencial de redução e otimização dos custos do ciclo de vida do sistema de segurança para a instalação. Os custos do ciclo de vida da alternativa mais econômica chegam a ser cerca de 97% menores do que os custos da alternativa mais simples proposta. É importante destacar que a redução de custos é obtida considerando os acréscimos nos custos de investimento e refere-se a uma vida útil da instalação de 30 anos.

Ficou evidenciado também pelos resultados apresentados que os maiores custos envolvidos no valor do custo do ciclo de vida das alternativas analisadas estão relacionados ao OPEX, dado que esta é a parcela que considera os custos da operação do sistema, ou seja, no caso estudado, os custos das paradas necessárias para testes do sistema de segurança, de forma a garantir o atendimento ao nível de confiabilidade requerido. A análise deste resultado permite concluir que, para o caso estudado, é bastante vantajoso o investimento na aquisição de equipamentos que levem a um menor número de paradas necessárias para testes do sistema de segurança, ou seja, o investimento representado pela parcela CAPEX traz um retorno extremamente vantanjoso para o custo do ciclo de vida (CCV) do sistema, devido à economia gerada na parcela do OPEX.

É importante ressaltar que toda a análise do CCV do sistema está baseada em dados típicos da indústria de processos e em dados disponíveis na literatura especializada e o critério utilizado é extremamente dependente dos valores das taxas de falhas e

dos custos. Em função disso, a robustez dos resultados obtidos foi uma preocupação durante o desenvolvimento deste trabalho. De forma a tentar verificar a consistência e validar os dados utilizados, realizou-se uma análise de sensibilidade com relação a alguns parâmetros críticos utilizados, como o coeficiente de diagnóstico de teste parcial, o custo das válvulas e o intervalo entre testes parciais. Os resultados obtidos validaram a robustez dos resultados obtidos (ver seção 6.8), em relação aos referidos parâmetros críticos.

Como resultado, em função dos resultados obtidos para as dez alternativas inicialmente propostas, obteve-se a alternativa "**FIS E-2***" (redundância em todos os elementos da FIS: transmissor de pressão (2oo3), CLP (*hot standby*) e válvula de bloqueio tipo 2 (1oo2), com a realização de testes parciais do atuador a cada 15 dias - ver Figura 7.1) como a que apresenta a melhor a relação custo-benefício, tendo em vista o valor do custo do ciclo de vida do sistema, conforme apresentado na Figura 7.2.

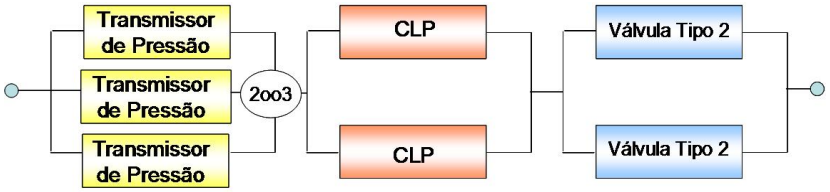


FIGURA 7.1: Alternativa FIS E-2*

Outro importante resultado deste trabalho está discutido e apresentado no Capítulo 5. A Norma IEC 61508 (IEC-61508-6 2000), além de indicar os métodos para a avaliação do SIL Requerido, fornece também várias equações para a avaliação quantitativa da PFD de várias configurações de sistemas de segurança, sem no entanto, apresentar as correspondentes deduções destas expressões apresentadas, nem sequer explicitar as premissas e aproximações usadas para se chegar às equações para cada uma das configurações de SIS.

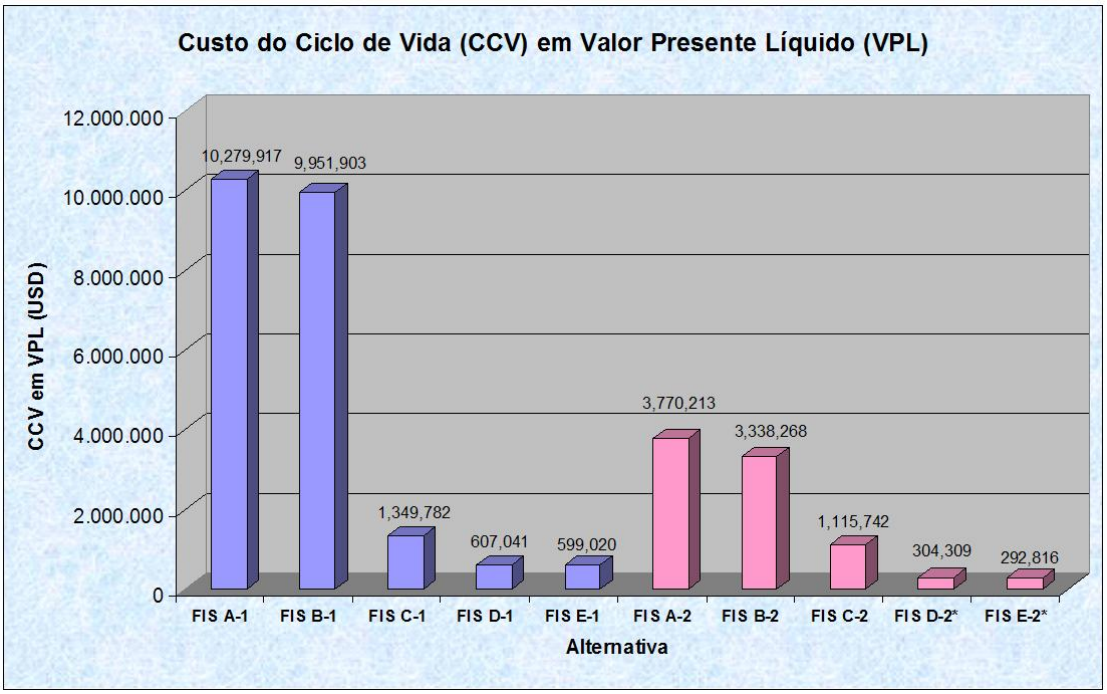


FIGURA 7.2: Gráfico do Custo do Ciclo de Vida e Alternativas Analisadas

Neste trabalho foram apresentadas as deduções formais das equações das PFDs das várias configurações apresentadas na referência citada, evidenciando de forma clara, as principais premissas e aproximações embutidas nas mesmas, permitindo inclusive considerar testes parciais do sistema de segurança; apresentou também a dedução correspondente para uma configuração *koon* qualquer. Portanto, pode-se dizer que este trabalho esclareceu alguns conceitos básicos que estão por trás das expressões apresentadas na Norma IEC 61508, generalizando-as para outras configurações, bem como forneceu exemplos práticos ilustrando os seus usos e os efeitos das restrições impostas pela norma para se alcançar o nível de SIL Requerido com algumas configurações.

## 7.2 Propostas para Trabalhos Futuros

Como possíveis extensões do trabalho aqui apresentado, sugere-se:

- a proposição de uma formulação analítica para cálculo da PFD para uma configuração *koon* qualquer considerando a possibilidade de testes parciais ou imperfeitos.

- a comparação dos resultados das equações analíticas baseadas nas aproximações

lineares (propostas pela Norma IEC 61508) com os resultados das integrações numéricas das equações exatas (sem as aproximações consideradas) para o cálculo da probabilidade de falha na demanda.

- refinamento dos dados utilizados para o cálculo do custo do ciclo de vida, recomendando inclusive que empresas ou órgãos interessados em análises semelhantes mantenham as informações (dados econômicos ou de confiabilidade) armazenadas na forma de banco de dados, de forma a facilitar uma rápida avaliação das várias alternativas para um projeto envolvendo equipamentos de segurança.

Outras possibilidades de extensão a serem exploradas em futuros trabalhos seriam:

- a ampliação das alternativas analisadas com a inclusão de configurações de CLPs mais sofisticados como os TMR´s (ou triplex) e os QMR's (tipo 2oo4).

- o refinamento da análise custo-benefício, por exemplo, com a inclusão dos custos para a realização dos testes, ou ainda, com a avaliação dos efeitos da realização dos testes completos durante o período de parada geral da planta.

# Referências Bibliográficas


AIChE (1993), *Guidelines for Safe Automation of Chemical Process*, American Institute of Chemical Engineers, Center for Chemical Process Safety (CCPS), New York, USA.

AIChE (2001), *Layers of Protection Analysis, Simplified Process Risk Assessment*, American Institute of Chemical Engineers, Center for Chemical Process Safety (CCPS), New York, USA.

ALVARENGA, T. V. (2005), *Metodologia de Análise de RAM (Reliability, Availability and Maintainability) por Simulação Baseada em Eventos Discretos Aplicada à Indústria Offshore como Suporte à Decisão Gerencial*, Dissertação de M.Sc., Universidade Federal Fluminense, Niterói, Rio de Janeiro.

ANDREWS, J. D. & MOSS, T. (2002), *Reliability and Risk Assessment*, $2^a$ ed., The American Society of Mechanical Engineers, ASME PRESS, New York, USA.

ANSI/API-521 (1997), *Guide for Pressure Relieving and Depressuring Systems*, API - American Petroleum Institute, USA.

ANSI/ISA-84.00.01 (2004), *Functional Safety: Safety Instrumented System for the Process Industry Sector - Parts 1, 2 and 3*, ISA - The Instrumentation, Systems, and Automation Society, Research Triangle Park, North Carolina, USA.

ASME (1996), *Code Case 2211 of ASME - Section VIII*, ASME - American Society of Mechanical Engineers, USA.

ASME-BPCV-VIII (2004), *Boiler and Pressure Vessel Code, Section VIII - Rules for Construction of Pressure Vessels*, ASME - American Society of Mechanical Engineers, New York, USA, New York, USA.

BECKMAN, L. & CAPECCHI, P. (2002), 'Determinando o Nível de Integridade de Segurança para seu processo', *Revista InTech, Fevereiro* pp. 30–32.

BEGA, E. A., DELMÉE, G. J., COHN, P. E., BULGARELLI, R., KOCH, R. & FINKEL, V. S. (2003), *Instrumentação Industrial*, Instituto Brasileiro de Petróleo e Gás - IBP, 1a edição, Editora Interciência, Rio de Janeiro.

BEURDEN, I. V. & BEURDEN-AMKREUTZ, R. V. (2004), 'What does proven in use imply?', *ISA 2004, Houston, Texas, USA, 5-7 Outubro* .

CHAME, L. M. & OLIVEIRA, L. F. S. (2006), *ORBIT SIL User Guide and Technical Manual*, Revisão 0, Det Norske Veritas, Rio de Janeiro.

CHAME, L. M., OLIVEIRA, L. F. S. & DINIZ, F. L. B. (2007), 'Alternativas para o atendimento ao SIL requerido em Plantas de Processo', *IBP - IV Congresso Rio Automação 2007, Rio de Janeiro, 09-10 Março* (IBP-53707).

DIN-VDE-19250 (1998), *Measurement and Control, Fundamental Safety Aspects for Measuring and Control Protective Equipment*, Berlin, Germany.

DINIZ, F. L. B. (1997), *Análise da Confiabilidade de um Sistema de Automação pela Combinação dos Métodos de Markov e de Árvore de Falhas*, Dissertação de M.Sc., Universidade Federal da Bahia, Bahia.

ERIKSEN, R., HARMS, J. & MCDONNELL, R. (1999), *Assessing the Reliability of Dynamic Positioning Systems for Deepwater Drilling Vessels*, Technical report, Det Norske Veritas, Norway.

ERIKSEN, R. & SAUCIER, B. (2000), 'Selecting Cost-Effective and Safe Deepwater Completion Tieback Alternatives', *Offshore Technology Conference - Houston, Texas, USA* (OTC 12167).

FLEMING, K. N. (1975), 'A Reliability Model for Common Mode Failure in Redundant Safety System', *Proceedings of the Sixth Annual Pittsburgh Conference on Modeling and Simulation* .

FRANCISCO, A. S. (1993), *Análise de Confiabilidade de Configurações Alternativas de Controladores Lógicos Programáveis para Sistemas de Segurança*, Dissertação de M.Sc., Universidade Federal do Rio de Janeiro, Rio de Janeiro.

GAMAL, H. (1993), *Análise de Custo-Benefício de Arquiteturas de CLPs Tolerantes a Falhas Utilizadas em Sistemas de Proteção*, Dissertação de M.Sc., Universidade Federal do Rio de Janeiro, Rio de Janeiro.

GOBLE, W. M. (1998), *Control System Safety Evaluation and Reliability: Techniques and Applications*, $2^a$ ed., ISA - The Instrumentation, Systems and Automation Society, Research Triangle Park, North Carolina, USA.

GOBLE, W. M. & BEURDEN, I. V. (2002), 'Safety Integrity Level Verification via Quantitative Reliability Calculations', *ISA - The Instrumentation, Systems and Automation Society* .

GOBLE, W. M. & CHEDDIE, H. L. (2005), *Safety Instrumented Systems Verification: Practical Probabilist Calculations*, ISA - The Instrumentation, Systems and Automation Society, Research Triangle Park, North Carolina, USA.

GRUHN, P. (2002), 'Safety Instrumented System Verification Using Simplified Equations', *ISA Safety Instrumented Systems for the Process Industries Conference, Baltimore, MD, USA* .

GRUHN, P. (2004), 'Different SIL (Safety Integrity Level) Selection Techniques can yield significantly different answers', *ISA Automation West, USA* .

GRUHN, P. & FINKEL, V. S. (2002), 'Os Sistemas de Segurança e a Falácia de ´´Quanto mais redundância, melhor"', *Revista InTech, Fevereiro* pp. 34–36.

HAUGE, S., HOKSTAD, P., LANGSETH, H. & OIEN, K. (2006), *Reliability Prediction Method for Safety Instrumented Systems - PDS Method Handbook*, In: SINTEF Report STF50 A06031, Ed. 2006 , SINTEF Technology and Society, PDS, Trondheim, Noruega.

HAUGE, S., LANGSETH, H. & ONSHUS, T. (2006), *Reliability Data for Safety Instrumented Systems - PDS Data Handbook*, In: SINTEF Report STF50 A06030, SINTEF Technology and Society, Trondheim, Norway.

IEC-61078 (2006), *Analysis Techniques for Dependability - Reliability Block Diagram and Boolean Methods*, $2^a$ ed., IEC - International Electrotechnical Commission, Geneva, Switzerland.

IEC-61508 (1998), *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, Parts 1-7*, $1^a$ ed., IEC - International Electrotechnical Commission, Geneva, Switzerland.

IEC-61508-1 (1998), *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 1: General Requirements*, $1^a$ ed., IEC - International Electrotechnical Commission, Geneva, Switzerland.

IEC-61508-2 (2000), *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 2: Requirements for E/E/PE Safety-Related System*, $1^a$ ed., IEC - International Electrotechnical Commission, Geneva, Switzerland.

IEC-61508-3 (1998), *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 3: Software Requirements*, $1^a$ ed., IEC - International Electrotechnical Commission, Geneva, Switzerland.

IEC-61508-4 (1998), *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 4: Definitions and abbreviations*, $1^a$ ed., IEC - International Electrotechnical Commission, Geneva, Switzerland.

IEC-61508-5 (1998), *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 5: Examples of Methods for determination of Safety Integrity Levels*, $1^a$ ed., IEC - International Electrotechnical Commission, Geneva, Switzerland.

IEC-61508-6 (2000), *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems - Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3*, $1^a$ ed., IEC - International Electrotechnical Commission, Geneva, Switzerland.

IEC-61511 (2003), *Functional Safety - Safety Instrumented Systems for the Process Industry Sector*, $1^a$ ed., IEC - International Electrotechnical Commission, Geneva, Switzerland.

KLEIN, K. L. (2005), 'Grandfathering, it's not about being old, it's about being safe', *The Instrumentation, Systems, and Automation Society - ISA EXPO 2005* **McCormick Place Lakeside Center, Chicago, Illinois, USA, 25-27 Outubro**.

LAFRAIA, J. R. B. (n.d.), *Manual de Confiabilidade, Mantenabilidade e Disponibilidade*, 1ª ed., Qualitymark, Universidade Petrobras, Rio de Janeiro.

LAYER, T. J. (2004), 'Selecting "Sensors" for Safety Instrumented Systems per IEC 61511 (ISA 84.00.01 - 2004)', *ISA AUTOMATION WEST, ISA - The Instrumentation, Systems and Automation Society* .

LIMA, M. C. (2002), *Análise do Potencial de Falhas Humanas em Atividades de Manutenção*, Dissertação de M.Sc., Universidade Federal Fluminense, Niterói, Rio de Janeiro.

MAGGIOLI, V. (1999), 'Overview and Status of IEC 61511 Functional Safety: Safety Instrumented System for the Process Sector', *ISA - The Instrumentation, Systems and Automation Society* .

MARSZAL, E. M. & MITCHELL, K. J. (2003), 'Defining Safety Instrumented Functions', *ISA - The Instrumentation, Systems, and Automation Society* .

MARSZAL, E. M. & SCHARPF, E. W. (2002), *Safety Integrity Level Selection: Systematic Methods Including Layer of Protection Analysis*, ISA - The Instrumentation, Systems and Automation Society, Research Triangle Park, North Carolina, USA.

MOSLEH, A., RASMUSON, D. M. & MARSHALL, F. M. (1998), *Guidelines on Modeling Common-Cause Failures in Probabilistic Risk Assessment*, NUREG/CR-5485, U. S. Nuclear Regulatory Commission.

NR-13 (1994), *Norma Regulamentadora NR-13: Caldeiras e Vasos de Pressão*, MTE - Ministério do Trabalho e Emprego.

OLF (2004), *Application of IEC 61508 and IEC 61511 in the Norwegian Petroleum Industry*, Relatório Técnico 070, The Norwegian Oil Industry Association, Norway.

OLIVEIRA, L. F. S. (n.d.), Introdução à Engenharia da Confiabilidade de Sistemas.

OLIVEIRA, L. F. S. & FLEMING, P. V. (1997), 'Introdução à Engenharia de Confiabilidade'.

OLIVEIRA, L. F. S., MELO, P. F. F. F., FLEMING, P. V. & LIMA, J. E. P. (1985), 'Introdução à Análise de Segurança por árvore de Falhas', *COPPE/UFRJ* .

OREDA (2002), *Offshore Reliability Data Handbook*, 4ª ed., OREDA Participants, SINTEF Industrial Management, Norway.

PEREIRA, S. B. & ALIPERTI, J. (2006), 'Normas da ISA: O Mundo da Instrumentação, Automação e Controle na Palma das Mãos', *Revista InTech* (n. 79, Jan), pp. 25–30.

PETROBRAS (2002), *N-2595 - Critérios de Projeto e Manutenção para Sistemas Instrumentados de Segurança em Unidades Industriais*, PETROBRAS, CONTEC (Comissão de Normas Técnicas), Revisão B/Out 2002, Rio de Janeiro.

ROQUE, J. C. D. M. (2006), 'Conceitos de Segurança Funcional: Normas IEC 61508/61511/62062', *Revista Petro e Química, Abril* (283), páginas 86–90.

SANT´ANA, M. C. (2006), *Uma Modelagem das Incertezas Associadas a Falhas de Causa Comum considerando Diversidade e Envelhecimento*, Dissertação de M.Sc., Universidade Federal do Rio de Janeiro, Rio de Janeiro.

SMITH, D. J. & SIMPSON, K. G. L. (2004), *Functional Safety: a Straightforward guide to applying IEC 61508 and related Standards*, $2^a$ ed., Elsevier Butterworth-Heinemann, Great Britain.

SUMMERS, A. E. (2002), 'What every Manager should know about the new SIS Standards', *ISA Safety Instrumented Systems for the Process Industries Conference, Baltimore, MD, USA, 14-16 Maio* .

SUMMERS, A. E. & ZACHARY, B. A. (2002), 'Partial Stroke Testing and SIF Performance', *ISA 2002 Technical Conference Paper, Chicago, IL, USA, 21-24 Outubro* .

# Apêndice A

# Cálculo da PFD para Arquiteturas mais usuais usando a IEC 61508

## A.1 Introdução

A seção 5.7 desta dissertação apresentou a dedução de uma expressão para cálculo da probabilidade de falha na demanda (PFD) para um sistema *koon* qualquer, baseado nas expressões apresentadas na Norma IEC 61508 (ver referência (IEC-61508-6 2000)). O objetivo desta dedução foi poder proporcionar ao usuário desta metodologia a aplicação do modelo de cálculo apresentado pela referenciada norma, para qualquer configuração *koon* existente em seu sistema, e não apenas para as arquiteturas apresentadas pela norma: 1oo1, 1oo2, 1oo2D, 2oo2 e 2oo3.

Conforme visto anteriormente, a PFD de um sistema de proteção qualquer pode ser expressa como o produto da freqüência média de ocorrência do estado falho pela duração média da permanência neste estado, ou seja:

$$PFD = \phi \cdot T \tag{A.1}$$

onde $\phi$ é a freqüência média de ocorrência de uma falha crítica do sistema em um dado período de tempo e $T$ é o tempo médio de permanência neste estado.

Desta forma, a seguir são apresentadas as expressões desenvolvidas para o cálculo de cada uma destas parcelas para um sistema *koon* qualquer e de forma a validar alguns dos resultados apresentados na seção 5.6, são também apresentados os resultados do uso

destas expressões para algumas das arquiteturas mais usuais dos sistemas de segurança.

## A.2 Freqüência Média $\phi_{koon}$

Sendo $\phi$ dado conforme a equação A.2 abaixo:

$$\phi_{koon} = \frac{n!}{(k-1)!(n-k+1)!}\lambda^{n-k+1}T_1^{n-k} \tag{A.2}$$

é possível dizer que:

- $\phi_{1oo1} = \frac{1!}{0!1!}\lambda T_1^0 = \lambda$
- $\phi_{1oo2} = \frac{2!}{0!2!}\lambda^2 T_1 = \lambda^2 T_1$
- $\phi_{2oo2} = \frac{2!}{1!1!}\lambda T_1^0 = 2\lambda$
- $\phi_{2oo3} = \frac{3!}{1!2!}\lambda^2 T_1 = 3\lambda^2 T_1$
- $\phi_{1oo3} = \frac{3!}{0!3!}\lambda^3 T_1^2 = \lambda^3 T_1^2$
- $\phi_{3oo3} = \frac{3!}{2!1!}\lambda^1 T_1^0 = 3\lambda$
- $\phi_{1oo4} = \frac{4!}{0!4!}\lambda^4 T_1^3 = \lambda^4 T_1^3$
- $\phi_{2oo4} = \frac{4!}{1!3!}\lambda^3 T_1^2 = 4\lambda^3 T_1^2$
- $\phi_{3oo4} = \frac{4!}{2!2!}\lambda^2 T_1^1 = 6\lambda^2 T_1$
- $\phi_{4oo4} = \frac{4!}{3!1!}\lambda^1 T_1^0 = 4\lambda$

## A.3 Tempo Médio no Estado Falho $T_{koon}$

Sendo $T_{koon}$, o valor médio do tempo que o sistema *koon* permanece no estado falho, dado conforme a equação A.3 a seguir:

$$T_{koon} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{n-k+2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR \tag{A.3}$$

é possível dizer que:

- $T_{1oo1} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR)\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR$
- $T_{1oo2} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR)\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR$
- $T_{2oo2} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR)\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR$
- $T_{2oo3} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR)\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR$
- $T_{1oo3} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{4} + MTTR)\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR$
- $T_{3oo3} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR)\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR$
- $T_{1oo4} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{5} + MTTR)\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR$
- $T_{2oo4} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{4} + MTTR)\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR$
- $T_{3oo4} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR)\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR$
- $T_{4oo4} = \frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR)\right) + \frac{\lambda_{DD}}{\lambda_D}MTTR$

## A.4 Probabilidade de Falha na Demanda $PFD_{koon}$

### A.4.1 $PFD_{koon}$

A equação 5.66, apresentada na seção 5.7, está reproduzida abaixo e apresenta o valor da PFD para um sistema *koon* qualquer, sem considerar a contribuição do reparo ou de falhas de modo comum.

$$PFD_{koon} = \frac{n!}{(k-1)!(n-k+2)!}\lambda^{n-k+1}T_1^{n-k+1} = \frac{n!}{(k-1)!(n-k+2)!}(\lambda T_1^{n-k+1}) \tag{A.4}$$

desta forma, é possível dizer que:

- $PFD_{1oo1} = \frac{1!}{(0)!(1-1+2)!}(\lambda T_1^{1-1+1}) = \frac{1}{2}\lambda T_1$
- $PFD_{1oo2} = \frac{2!}{(0)!(2-1+2)!}(\lambda T_1^{2-1+1}) = \frac{1}{3}\lambda T_1^2$
- $PFD_{2oo2} = \frac{2!}{(1)!(2-2+2)!}(\lambda T_1^{2-2+1}) = \lambda T_1$
- $PFD_{2oo3} = \frac{3!}{(1)!(3-2+2)!}(\lambda T_1^{3-2+1}) = \lambda T_1^2$

- $PFD_{1oo3} = \frac{3!}{(0)!(3-1+2)!}(\lambda T_1^{3-1+1}) = \frac{1}{4}\lambda T_1^2$
- $PFD_{3oo3} = \frac{3!}{(2)!(3-3+2)!}(\lambda T_1^{3-3+1}) = \frac{3}{2}\lambda T_1$
- $PFD_{1oo4} = \frac{4!}{(0)!(4-1+2)!}(\lambda T_1^{4-1+1}) = \frac{1}{5}\lambda T_1^4$
- $PFD_{2oo4} = \frac{4!}{(1)!(4-2+2)!}(\lambda T_1^{4-2+1}) = \lambda T_1^3$
- $PFD_{3oo4} = \frac{4!}{(2)!(4-3+2)!}(\lambda T_1^{4-3+1}) = 2\lambda T_1^2$
- $PFD_{4oo4} = \frac{4!}{(3)!(4-4+2)!}(\lambda T_1^{4-4+1}) = 2\lambda T_1$

### A.4.2 $PFD_{koon}$ Considerando a Contribuição do Reparo

Conforme citado, a equação A.4 fornece a $PFD_{koon}$ sem considerar a contribuição do reparo para a indisponibilidade do sistema (somente a contribuição das falhas não detectadas durante o intervalo entre testes). Para incluir a contribuição do reparo, deve-se tomar o "tempo médio no estado falho" para o sistema *koon* dado pela equação A.3, ou seja, multiplicando esta equação pela equação A.2, chega-se a:

$$PFD_{koon} = \frac{n!}{(k-1)!(n-k+1)!}(\lambda_D^{n-k+1} T_1^{n-k}) \times \left[\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{n-k+2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR\right] \quad \text{(A.5)}$$

#### A.4.2.1 Arquitetura 1oo1

Fazendo $k = 1$ e $n = 1$ e substituindo na equação A.5, temos:

$$PFD_{1oo1} = \frac{1!}{(0)!(1)!}(\lambda_D^{1-1+1} T_1^{1-1}) \left[\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{1-1+2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR\right]$$

então:

$$PFD_{1oo1} = \lambda_D \underbrace{\left[\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR\right]}_{t_{CE}} \quad \text{(A.6)}$$

ou seja:

$$PFD_{1oo1} = \lambda_D t_{CE} \tag{A.7}$$

conforme apresentado na equação 5.20.

#### A.4.2.2 Arquitetura 1oo2

Fazendo $k = 1$ e $n = 2$ e substituindo na equação A.5, temos:

$PFD_{1oo2} = \frac{2!}{(0)!(2)!}(\lambda_D^{2-1+1} T_1^{2-1}) \left[\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2-1+2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR\right]$

então:

$$PFD_{1oo1} = \lambda_D^2 T_1 \underbrace{\left[\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR\right]}_{t_{GE}} \tag{A.8}$$

conforme visto anteriormente, $t_{CE} \cong \frac{T_1}{2}$, e sendo $t_{GE}$ dado conforme apresentado acima, chega-se a:

$$PFD_{1oo2} = 2\lambda_D^2 t_{CE} t_{GE} \tag{A.9}$$

conforme apresentado na equação 5.39.

#### A.4.2.3 Arquitetura 2oo2

Fazendo $k = 2$ e $n = 2$ e substituindo na equação A.5, temos:

$PFD_{2oo2} = \frac{2!}{(1)!(1)!}(\lambda_D^{2-2+1} T_1^{2-2}) \left[\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{2-2+2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR\right]$

ou seja:

$$PFD_{2oo2} = \lambda_D^2 T_1 \underbrace{\left[\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR\right]}_{t_{CE}} \tag{A.10}$$

então:

$$PFD_{2oo2} = 2\lambda_D t_{CE} \tag{A.11}$$

conforme apresentado na equação 5.46.

#### A.4.2.4 Arquitetura 2oo3

Fazendo $k = 2$ e $n = 3$ e substituindo na equação A.5, temos:

$$PFD_{2oo3} = \frac{3!}{(1)!(2)!}(\lambda_D^{3-2+1} T_1^{3-2}) \left[\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3-2+2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR\right]$$

ou seja:

$$PFD_{2oo3} = 3\lambda_D^2 T_1 \underbrace{\left[\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR\right]}_{t_{GE}} \tag{A.12}$$

conforme visto anteriormente, $t_{CE} \cong \frac{T_1}{2}$, e sendo $t_{GE}$ dado conforme apresentado acima, chega-se a:

$$PFD_{2oo3} = 6\lambda_D^2 t_{CE} t_{GE} \tag{A.13}$$

conforme apresentado na equação 5.57.

#### A.4.2.5 Arquitetura 1oo3

Fazendo $k = 1$ e $n = 3$ e substituindo na equação A.5, temos:

$$PFD_{1oo3} = \frac{3!}{(0)!(3)!}(\lambda_D^{3-1+1} T_1^{3-1}) \left[\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3-1+2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR\right]$$

ou seja:

$$PFD_{1oo3} = \lambda_D^3 T_1^2 \underbrace{\left[\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{4} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR\right]}_{T_{1oo3}} \tag{A.14}$$

e, conforme visto anteriormente, dado que $t_{CE} \cong \frac{T_1}{2}$, chega-se a:

$$PFD_{1oo3} = 4\lambda_D^3 t_{CE}^2 T_{1oo3} \tag{A.15}$$

#### A.4.2.6 Arquitetura 3oo3

Fazendo $k = 3$ e $n = 3$ e substituindo na equação A.5, temos:

$$PFD_{3oo3} = \frac{3!}{(2)!(1)!}(\lambda_D^{3-3+1} T_1^{3-3}) \left[\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3-3+2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR\right]$$

ou seja:

$$PFD_{3oo3} = 3\lambda_D T_1 \underbrace{\left[\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR\right]}_{t_{CE}} \tag{A.16}$$

então:

$$PFD_{3oo3} = 3\lambda_D t_{CE} \tag{A.17}$$

#### A.4.2.7 Arquitetura 1oo4

Fazendo $k = 1$ e $n = 4$ e substituindo na equação A.5, temos:

$$PFD_{1oo4} = \frac{4!}{(0)!(4)!}(\lambda_D^{4-1+1} T_1^{4-1}) \left[\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3-2+2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR\right]$$

ou seja:

$$PFD_{1oo4} = \lambda_D^4 T_1^3 \left[ \frac{\lambda_{DU}}{\lambda_D} \left( \frac{T_1}{5} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \right] \tag{A.18}$$

ou ainda:

$$PFD_{1oo4} = \lambda_D^3 T_1^3 \left[ \lambda_{DU} \left( \frac{T_1}{5} + MTTR \right) + \lambda_{DD} MTTR \right] \tag{A.19}$$

e, conforme visto anteriormente, dado que $t_{CE} \cong \frac{T_1}{2}$, chega-se a:

$$PFD_{1oo4} = 8\lambda_D^3 t_{CE}^3 \left[ \lambda_{DU} \left( \frac{T_1}{5} + MTTR \right) + \lambda_{DD} MTTR \right] \tag{A.20}$$

#### A.4.2.8 Arquitetura 2oo4

Fazendo $k = 2$ e $n = 4$ e substituindo na equação A.5, temos:

$$PFD_{2oo4} = \frac{4!}{(1)!(3)!} (\lambda_D^{4-2+1} T_1^{4-2}) \left[ \frac{\lambda_{DU}}{\lambda_D} \left( \frac{T_1}{4-2+2} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \right]$$

ou seja:

$$PFD_{2oo4} = 4\lambda_D^3 T_1^2 \left[ \frac{\lambda_{DU}}{\lambda_D} \left( \frac{T_1}{4} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \right] \tag{A.21}$$

e, conforme visto anteriormente, dado que $t_{CE} \cong \frac{T_1}{2}$, chega-se a:

$$PFD_{2oo4} = 16\lambda_D^3 t_{CE}^2 \underbrace{\left[ \frac{\lambda_{DU}}{\lambda_D} \left( \frac{T_1}{4} + MTTR \right) + \frac{\lambda_{DD}}{\lambda_D} MTTR \right]}_{T_{1oo3}} \tag{A.22}$$

note que $T_{1oo3}$ pode ser visto também na equação A.14. É possivel então verificar que:

$$PFD_{2oo4} = 16\lambda_D^3 t_{CE}^2 T_{1oo3} \tag{A.23}$$

#### A.4.2.9 Arquitetura 3oo4

Fazendo $k = 3$ e $n = 4$ e substituindo na equação A.5, temos:

$$PFD_{3oo4} = \frac{4!}{(2)!(2)!}(\lambda_D^{4-3+1} T_1^{4-3}) \left[\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{4-3+2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR\right]$$

ou seja:

$$PFD_{3oo4} = 6\lambda_D^2 T_1 \underbrace{\left[\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR\right]}_{t_{GE}} \tag{A.24}$$

conforme visto anteriormente, $t_{CE} \cong \frac{T_1}{2}$, e sendo $t_{GE}$ dado conforme apresentado acima, chega-se a:

$$PFD_{2oo3} = 6\lambda_D^2 2 t_{CE} t_{GE} \tag{A.25}$$

ou ainda:

$$PFD_{2oo3} = 12\lambda_D^2 t_{CE} t_{GE} \tag{A.26}$$

#### A.4.2.10 Arquitetura 4oo4

Fazendo $k = 4$ e $n = 4$ e substituindo na equação A.5, temos:

$$PFD_{4oo4} = \frac{4!}{(3)!(1)!}(\lambda_D^{4-4+1} T_1^{4-4}) \left[\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{4-4+2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR\right]$$

ou seja:

$$PFD_{4oo4} = \lambda_D^2 T_1 \underbrace{\left[\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{3} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR\right]}_{t_{CE}} \tag{A.27}$$

então:

$$PFD_{4oo4} = 4\lambda_D t_{CE} \tag{A.28}$$

### A.4.3 $PFD_{koon}$ Considerando a Contribuição do Reparo e Falhas de Causa Comum

Conforme citado, a equação A.5 fornece a $PFD_{koon}$ considerando a contribuição do reparo para a indisponibilidade do sistema, ou seja, o "tempo médio no estado falho" para o sistema *koon*. No entanto, também deve ser considerada a possibilidade de ocorrência de falhas comuns. A equação A.29 a seguir apresenta a equação para o cálculo da probabilidade de falha na demanda considerando tanto a contribuição do reparo quanto a probabilidade de falhas de causa comum.

$$\begin{aligned} PFD_{koon} = \left[\frac{n!}{(k-1)!(n-k+1)!}\left[(1-\beta_D)\lambda_{DD} + (1-\beta)\lambda_{DU}\right]^{n-k+1} T_1^{n-k}\right] \times \\ \left[\frac{\lambda_{DU}}{\lambda_D}\left(\frac{T_1}{n-k+2} + MTTR\right) + \frac{\lambda_{DD}}{\lambda_D} MTTR\right] + \beta_D \lambda_{DD} MTTR \\ + \beta\lambda_{DU}\left(\frac{T_1}{2} + MTTR\right) \end{aligned} \tag{A.29}$$