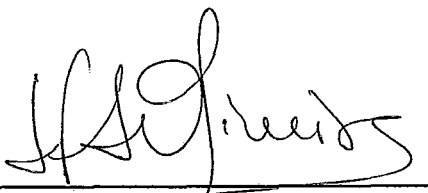
ANÁLISE DE CUSTO-BENEFÍCIO DE ARQUITETURAS DE CLPs TOLERANTES A FALHAS UTILIZADAS EM SISTEMAS DE PROTEÇÃO

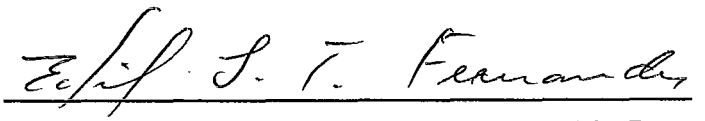
Haroldo Gamal

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

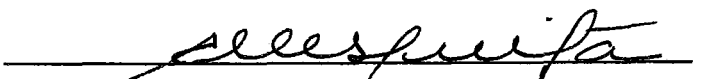
Aprovada por:



Prof. Luiz Fernando Seixas de Oliveira, Ph. D.
(Presidente)



Prof. Edil Severiano Tavares Fernandes, Ph. D.



Prof. Antônio Carneiro de Mesquita, Dr. Estado

RIO DE JANEIRO, RJ - BRASIL
ABRIL DE 1993

Gamal, Haroldo

Análise de Custo Benefício de Arquiteturas de CLPs Tolerantes a Falhas Utilizados em Sistemas de Proteção [Rio de janeiro] 1993

vii, 87p. 29,7 cm (COPPE/UFRJ, M. Sc., ENGENHARIA DE SISTEMAS E COMPUTAÇÃO, 1993)

Tese - Universidade Federal do Rio de Janeiro, COPPE

1. Arquitetura de Computadores 2. Confiabilidade

I. COPPE/UFRJ II. Título

I Wish You Were Here

(Roger Waters)

So, so you think you can tell Heaven from Hell, blue skies from pain.
Can You tell a green field from a cold steel rail? A smile from a veil?
Do you you think you can tell?

And did they get you to trade your heroes for ghosts ? Hot ashes for trees?
Hot air for a cool breeze? Cold commfort for change?
And did you exchange a walk on part in the war for a lead role in a cage?

How I wish, how I wish you were here.
We're just two lost souls swimming in a fish bowl, year after year,
Running over the same old ground. What have we found? The same old fears.
Wish you were here.

Resumo da Tese Apresentada à COPPE como parte dos requisitos necessários para a obtenção do grau de Mestre em Ciências (M. Sc.)

Análise de Custo Benefício de Arquiteturas de CLPs Tolerantes a Falhas Utilizados em Sistemas de Proteção
Abril de 1993

Orientador: Luiz Fernando Seixas de Oliveira
Programa: Engenharia de Sistemas e Computação

As técnicas de análise de confiabilidade permitem que os níveis de confiabilidade das alternativas para o projeto de um sistema de proteção sejam avaliados quantitativamente. Estess índices quantitativos obtidos na análise constituem-se em elementos importantes para o projetista, possibilitando o conhecimento das variações relativas de confiabilidade entre as diferentes alternativas 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 destes índicesnão se constitui em argumento suficiente para a tomada de decisão relativa à escolha de uma das alternativas consideradas. Portanto, 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 (ACB). O objetivo deste trabalho é a aplicação de uma técnica de Análise Custo-Benefício aplicada as alternativas de projeto de sistemas de proteção, utilizando diversas configurações de Controladores Lógicos Programáveis (CLPs) tolerantes a falha.

Abstract of Thesis presented to COPPE as partial fulfillment of the requirements for degree of Master of Science (M. Sc.)

Cost-Benefit Analisys of the PLC Architectures Fault-Tolerant Used in Protection Systems

April, 1993

Thesis Supervisor: Luiz Fernando Seixas de Oliveira
Departament: Programa de Engenharia de Sistemas e Computação

The utilization of reliability analysis technique permits that reliability levels of several alternate configurations for a given protection system design be evaluated. Undoubtly, the figures resulted from that aproach are very important for the designer, allowing the comparison among differents configutations, and for identifying de systems components contributing most for the failure probability. Otherwise, most of time, relative comparison among reliability results is not enough for decising the best configuration. So, as a rule of thumb, the decision process requires a comparison between costs and the related benefits. This comparison is the basic fundamental of a Cost-Benefit Analisys (CBA). The main goal of this study is the application of a Cost-Benefit Analisys technique to different configurations of a protection system constituted by Programmable Logic Controllers.

ÍNDICE

I. INTRODUÇÃO 1
I.1 - A Utilização de CLPs em Sistemas de Proteção 4
I.2 - Apresentação do Problema e Objetivos do Trabalho 4
I.3 - Organização da Tese 5

II. METODOLOGIA PARA AVALIAÇÃO DE CONFIABILIDADE E ANÁLISE CUSTO-BENEFÍCIO 6
II.1 - Introdução 6
II.2 - Conceitos de Confiabilidade de CLPs 7
II.2.1 - Disponibilidade 7
II.2.2 - Freqüência Esperada de Ocorrência 8
II.3 - Método Markoviano para Avaliação de Confiabilidade 9
II.3.1 - Fundamentos 9
II.3.2 - Matriz de Transição 10
II.3.3 - A matriz de taxas de transição 12
II.3.4 - Solução da equação básica 13
II.4 - Avaliação de Confiabilidade por Árvores de Falhas 13
II.5 - Análise Custo-Benefício 17
II.5.1 - Avaliação do Custo 17
II.5.2 - Avaliação do Benefício Esperado 18

III. ARQUITETURAS DE CLPs UTILIZADAS EM SISTEMAS DE PROTEÇÃO 20
III.1 - Introdução 20
III.2 - Descrição dos Equipamentos 21
III.2.1 - A Unidade de Processamento 22
III.2.2 - Sistema de Entrada e Saída 24
III.3 - Arquiteturas Redundantes de CLPs 25
III.2 - Configuração Simplex 26
III.4 - Configuração Dual-Dual 30
III.5 - Configuração Triplex 32

IV. MODELAGEM DO PROBLEMA E RESULTADOS OBTIDOS 36
IV.1 - Introdução 36
IV.2 - Modelagem das Configurações 36

IV.3 - Caso Exemplo: Sistema de Detecção de Incêndio em Plataformas Marítimas 41
IV.3.1 - Descrição do sistema de geração de sinais 41
IV.3.2 - Sistema de Detecção de Chama 42
IV.3.3 - Sistema Eletrônico de Detecção de Calor 42
IV.3.4 - Sistema de Detecção de Calor por Plug-fusíveis 43
IV.3.5 - Sistema de Acionamento Manual 43
IV.3.6 - Lógica de Acionamento do Painel de Fogo e Gás 44
IV.4 - Árvore de Falhas do Sistema de Detecção de Incêndio 44
IV.4.1 - Avaliação da Indisponibilidade Média 45
IV.4.2 - Avaliação da Freqüência de Acionamentos Espúrios 48
IV.4.3 - Dados de falhas 49
IV.5 - Análise Custo-Benefício 51
IV.5.1 - Avaliação dos Benefícios 51
IV.5.1 - Avaliação dos Custos 54
IV.5.3 - Resultados da análise 56

V. CONCLUSÕES E RECOMENDAÇÕES 61

BIBLIOGRAFIA 64

APÊNDICES 66
A. Árvore de Falhas de Indisponibilidade 67
B. Árvore de Falhas de Freqüência Espúria 74
C. Planilha Análise Custo-Benefício 80
D. Planilha de custo dos subsistemas de sensoramento 81
E. Determinação da freqüência de incêndio 82
E.1. Enfoque clássico 82
E.2. Enfoque bayesiano 84
F. Determinação das perdas devido a incêndio e falhas espúrias 86
F.1. Perdas humanas por incêndio 86
F.2. Perdas econômicas por incêndio 86
F.2. Perdas econômicas por falha espúria 87

I. INTRODUÇÃO

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. De um modo geral, a filosofia de prevenção a situações de emergência baseia-se na detecção das causas ainda no seu nascedouro, ou seja, tão logo os primeiros sinais de ocorrência possam ser identificados pelo sistema de proteção. Portanto, a confiabilidade desses sistemas, capazes de detectar situações de emergência ainda em fase incipiente, é de fundamental importância para manter o nível de risco dos trabalhadores dentro de limites aceitáveis e para garantir um nível adequado de proteção ao patrimônio da empresa.

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 de 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. Isto se deve às diferenças nos custos de implementação, operação e manutenção que normalmente existem entre diferentes configurações de um sistema. 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 (ACB).

Em se tratando de sistemas de segurança, os benefícios estão relacionados à redução do número de acidentes na instalação, com a 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 de 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 dos 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.

No caso dos sistemas de proteção, os benefícios obtidos com a melhoria da confiabilidade de sistemas estão intimamente ligados à redução dos riscos de vida para o pessoal e dos riscos de perdas econômicas associadas aos danos causados aos equipamentos (e estruturas) e às paradas de produção.

Embora conceitualmente simples, a realização de uma Análise Custo-Benefício enfrenta vários problemas relacionados tanto à quantificação dos benefícios como dos custos associados a cada alternativa. Sem dúvida, em se tratando de uma decisão envolvendo um sistema de segurança, a principal dificuldade está no estabelecimento de um "valor monetário para a vida humana", o qual deve ser mais precisamente definido como "os gastos que podem ser justificáveis para se evitar a ocorrência de uma morte estatisticamente esperada".

Embora possa parecer chocante para algumas pessoas, este julgamento é feito a todo instante em decisões envolvendo a implementação de sistemas de segurança. Por exemplo, o perigo de incêndio está sempre presente em qualquer edifício comercial, pondo em risco a vida dos seus ocupantes. Em função deste perigo, os edifícios comerciais modernos estão equipados com sistemas de detecção e combate a incêndios. Além disto, o Corpo de Bombeiros possui também inúmeros equipamentos para serem usados em casos de incêndio. No entanto, a existência destes sistemas não garante um nível de risco zero para os ocupantes dos prédios, o qual nunca pode ser atingido. Isto implica que os ocupantes estão sujeitos a um certo nível de risco, chamado risco residual, o qual decorre da probabilidade de falha dos sistemas de segurança quando da ocorrência de um incêndio no prédio. Pode-se, portanto, estimar o número de vítimas fatais em função de acidentes no prédio. Certamente, que um aumento da confiabilidade dos sistemas de segurança, por exemplo, através do aumento

da redundância dos mesmos, implicaria em uma redução do número de mortes estatisticamente esperado devido a acidentes no prédio. A questão que se coloca então, é a seguinte: "por que os responsáveis pela segurança do prédio não aumentam o nível de confiabilidade dos sistemas de segurança?" A resposta está certamente relacionada aos custos envolvidos nesta medida. A melhoria da confiabilidade dos sistemas implica em um custo adicional, o qual é julgado "desnecessário" ou "inadequado" pelos responsáveis, o que, em última análise, significa que o custo envolvido para se evitar a ocorrência de mais uma morte estatisticamente esperada é considerado muito alto. Tendo em vista que os recursos socialmente disponíveis para a redução dos riscos são finitos, este processo de decisão é inevitável. A novidade é que na Análise Custo-Benefício esta questão é colocada de uma forma explícita e não apenas implicitamente como vinha sendo feito até então. De acordo com trabalhos publicados por Jones-Lee (1976), por Mooney (1977) e pelo National Radiological Board da Inglaterra, pode-se concluir que os valores monetários para a vida humana utilizados em análises custo-benefício em inúmeras áreas de atividade têm variado entre trezentos mil e dez milhões de dólares, sendo este último o valor tradicionalmente utilizado em trabalhos na área da indústria nuclear.

Em relação à dificuldade envolvida na fixação do valor referido no parágrafo anterior, pode parecer que a avaliação dos demais valores relativos aos custos e benefícios seria muito fácil. No entanto, isto não é necessariamente verdadeiro. Existem inúmeros fatores que podem tornar este processo de quantificação bastante complicado. Por exemplo, uma conseqüência de um grande acidente industrial é que a imagem e a reputação da empresa envolvida podem ser seriamente afetadas (os casos da Union Carbide devido ao acidente de Bhopal e o da Exxon devido ao acidente no Alaska são exemplos clássicos). Este tipo de publicidade adversa e perda de boa vontade e de confiança por parte de clientes, empregados, acionistas, etc, podem ter um profundo impacto sobre a empresa, o qual é quase impossível de ser avaliado quantitativamente a priori. Tipicamente, este tipo de perda indireta é considerada como um "intangível" e excluída da análise de custo-benefício formal. No entanto, pode vir a se constituir em um importante fator no processo de tomada de decisão.

Outra dificuldade da realização de uma análise custo-benefício está na obtenção dos vários custos envolvidos (reposição ou reparos de equipamentos, custos de operação, custos de manutenção), na maior parte das vezes, em função da inexistência de uma sistema organizado de registro destes

dados pela empresa.

I.1 - A Utilização de CLPs em Sistemas de Proteção

A utilização de controladores lógicos programáveis (CLPs) aumentou significativamente na década de 80 em vários setores industriais. Originalmente desenvolvidos para substituir ou complementar os complexos sistemas de controle eletro-mecânicos existentes na indústria automobilista, os CLPs tiveram seu uso estendido desde tarefas relativamente simples (tais como, controle básico de máquinas, comunicação com sistemas de gerenciamento de informações, etc), até sofisticados sistemas de controle de processo.

Até bem recentemente, havia uma forte resistência de alguns setores (particularmente, de órgãos regulatamentadores e de empresas de seguro industrial) ao emprego de CLPs em sistemas de intertravamento de segurança, em substituição aos sistemas tradicionais de relés. A origem desta resistência estava no reconhecimento da dificuldade em se garantir as características de "falha segura" ("fail safe") do sistema, em função do pouco conhecimento acumulado sobre os modos de falha dos componentes e seus efeitos sobre o sistema. Esta dificuldade colocava-se em contraste ao completo domínio do comportamento de sistemas de intertravamento baseados em relés e temporizadores. Devido ao uso industrial crescente, com o conseqüente acúmulo de experiência operacional, e ao contínuo aperfeiçoamento dos CLPs, a utilização destes equipamentos em sistemas de intertravamento tem tido uma aceitação cada vez mais favorável da parte dos setores opositores mencionados acima. Um outro fator que tem contribuído significativamente para esta maior aceitação é a possibilidade de se projetar configurações com um alto grau de redundância (dual-simplex, dual-dual, triplex, redundância modular tripla, etc).

I.2 - Apresentação do Problema e Objetivos do Trabalho

Este trabalho será a aplicação de uma técnica de análise, que tem sido referida como "Análise Custo-Benefício", ou também como "Análise Custo-Risco-Benefício" (daqui para adiante será usada a primeira denominação por uma questão de simplicidade), aplicada às alternativas de projeto de sistemas de proteção, utilizando diversas configurações de Controladores Lógicos

Programáveis (CLPs) tolerantes a falhas.

Para a realização da análise, serão consideras quatro configurações básicas de CLPs, que serão descritas adiante, compondo, juntamente com uma malha de sensores, um sistema de proteção. Como exemplo de sistema de proteção, será usada a malha de detecção de incêndio de uma zona de produção de óleo de uma plataforma marítima. Os custos do sistema, incluindo a malha de sensores e CLPs, serão levantados a partir do "hardware" envolvido. Para o cálculo dos benefícios proporcionados pelo sistema de proteção, serão utilizadas ferramentas de cálculo de confiabilidade e dados internacionais.

I.3 - Organização da Tese

No Capítulo II, serão apresentados os conceitos e técnicas disponíveis para a avaliação dos atributos de confiabilidade envolvidos na análise, bem como a metodologia empregada na Análise de Custo-Benefício.

No Capítulo III serão apresentadas as configurações de Controladores Lógicos Programáveis a serem analisadas, descrevendo o "hardware", arquitetura e mecanismos de funcionamento de cada uma delas.

No Capítulo IV serão apresentados a modelagem empregada na avaliação de confiabilidade das configurações de CLPs, o caso exemplo a ser examinado e o resultados da análise de custo benefício.

No Capítulo V serão apresentados as conclusões finais deste trabalho.

II. METODOLOGIA PARA AVALIAÇÃO DE CONFIABILIDADE E ANÁLISE CUSTO-BENEFÍCIO

II.1 - Introdução

A idéia de tolerância a falhas, principalmente em sistemas eletrônicos, certamente não é uma idéia nova. Devido ao baixo nível de confiabilidade de seus componentes, os primeiros computadores fizeram uso ostensivo de técnicas de detecção de falhas Carter e Bouricius (1971). Na década de 50, alguns dos primeiros computadores da Bell Relay Computers (BRC), empregaram duas unidades paralelas de processamento, que se intercambiavam quando uma falha era detectada na unidade em operação. Na mesma época, começaram a surgir equipamentos que faziam teste de paridade, durante as operações de transferência de dados.

O surgimento do transistor, e seus níveis superiores de confiabilidade, conduziu a um período de decrescimento à computação tolerante a falha. Durante muito tempo a preocupação dos projetistas era de aumentar a velocidade e o poder computacional dos processadores. Nesta época acreditava-se que era suficiente aumentar a confiabilidade dos transistores para garantir o funcionamento correto dos computadores. Com o passar do tempo as máquinas foram ganhando espaço e, cada vez mais, operando sistemas mais complexos e cruciais. Para garantir que suas máquinas operassem corretamente durante um grande período de tempo, alguns fabricantes optaram por implementar arquiteturas com estruturas redundantes e usando métodos de detecção de falhas (Kuehen, 1969).

A John von Neumann foi creditado o primeiro trabalho em computação tolerante a falha. Em 1952, von Neumann apresentou uma série de trabalhos sobre o uso de unidades lógicas replicadas. Mais tarde, seria apresentado por ele um trabalho von Neumann (1956) em que mostraria o conceito de votação majoritária, e o impacto de sua utilização na probabilidade de falha de sistemas em apresentar resultados corretos.

Até os dias de hoje, apesar da dependência cada vez mais aguda do homem em relação a sistemas de informação, o campo da computação tolerante a falha ainda está numa fase relativamente embrionária. Os equipamentos com melhores características de confiabilidade ainda não estão disponíveis aos

usuários comuns. Hoje, estes equipamentos destinam-se a aplicações militares ou de segurança. Com a evolução das técnicas de VLSI, espera-se que os circuitos de nova geração possam garantir um nível superior de confiabilidade.

Obviamente, os sistemas utilizando Controladores Lógicos Programáveis, e que na verdade são sistemas de computação, quando empregados em sistemas de segurança exigem um nível maior de confiabilidade. Neste capítulo serão mostrados alguns conceitos de confiabilidade aplicados aos CLPs e algumas técnicas para sua avaliação. Ao final é apresentada a técnica de Análise Custo-Benefício.

II.2 - Conceitos de Confiabilidade de CLPs

A confiabilidade é avaliada por intermédio de ferramentas matemáticas e probabilísticas. Existem dois enfoques analíticos genéricos que podem ser usados para a modelagem de um sistema e a avaliação de sua confiabilidade. O primeiro é o chamado "enfoque indutivo", onde a partir de casos individuais procura-se uma generalização. Os métodos baseados neste enfoque partem da decomposição do sistema em suas partes, verificando-se, em seguida, os efeitos decorrentes de falhas destas partes sobre o sistema como um todo. O outro é o "enfoque dedutivo", que parte do caso geral e busca o específico. Este enfoque assemelha-se a um processo de investigação, onde a partir da falha do sistema, procuram-se as causas.

Os atributos a serem avaliados pela análise de confiabilidade devem ser escolhidos de acordo com a aplicação específica a que eles se destinam. Dentre os exemplos de atributos de confiabilidade podemos destacar: freqüência esperada de falha, o tempo médios entre falhas, a confiabilidade, a disponibilidade e a manutenibilidade. Para fins deste trabalho, os atributos necessários, bem como suas definições, estão apresentados abaixo.

II.2.1 - Disponibilidade

A Disponibilidade Instantânea é definida como a probabilidade de que um sistema estará funcionando num determinado instante de tempo t. Este atributo fornece uma medida da probabilidade do sistema estar disponível (ou

seja, apresentar condições de operar corretamente) quando demandado.

Em sistemas onde falhas não reveladas podem ocorrer, como aqueles que estão em situação de reserva ou "stand-by", a disponibilidade é expressa como uma média da disponibilidade instantânea no período T em que o sistema está em "stand-by", ou seja:

$$A_v = \frac{1}{T}\int_0^T A(t)\,dt \qquad \text{(II.1)}$$

onde:

$$A(t) = e^{-\lambda t} \qquad \text{(II.2)}$$

sendo λ a taxa de falhas do sistema.

Para a realização da Análise Custo-Benfício será necessário calcular a indisponibilidade do CLP, a qual corresponde a probabilidade de que os sistemas de segurança ou proteção não sejam acionados em uma situação de emergência devido a uma falha do CLP.

II.2.2 - Freqüência Esperada de Ocorrência

A Freqüência Esperada de Ocorrência reflete o número médio de vezes em que o sistema falha por unidade de tempo. Este atributo pode ser usado, geralmente, para avaliar os prejuízos econômicos que um dado tipo de falha causa durante um determinado período de tempo.

Conceitualmente, a freqüência pode ser determinada pelo produto de uma probabilidade, do sistema estar em determinada condição ou estado, por uma taxa de falha. Assim a freqüência média pode ser avaliada por:

$$\phi = P_m \cdot \lambda \qquad \text{(II.3)}$$

onde:

P_m = Probabilidade média do sistema estar em um determinado estado; e

λ = taxa de falha ou de demanda do sistema.

Para a realização da Análise Custo-Benefício, será calculada a **Freqüência de Acionamentos Espúrios** que corresponde à freqüência de ocorrência de acionamentos do sistema de segurança, controlado pelo CLP, devido a falhas intrínsecas do controlador, sem que haja uma real situação de emergência. Este tipo de falha causa o acionamento do aparato de segurança e proteção do processo que está sendo monitorado pelo equipamento.

II.3 - Método Markoviano para Avaliação de Confiabilidade

Dentre os métodos utilizados no cálculo de parâmetros 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. Em confiabilidade, um estado representa uma combinação de componentes, cada um dos quais num estado de falha ou funcionamento. Assim um sistema com n componentes, terá um espaço com, no máximo, $N=2^n$ estados. Com o passar do tempo, o sistema deverá evoluir caminhando entre esses estados. As falhas e reparos que os componentes sofrem com o passar do tempo, são os mecanismos de mudança de um estado para outro. As mudanças de estados são denominada transições.

II.3.1 - Fundamentos

O estado de um sistema num determinado instante de tempo pode ser representado por um vetor de dimensão n,

$$S(t) = \left[s_1, s_2, \ldots, s_n \right] \qquad \text{(II.4)}$$

onde s_i representa o estado do componente i no instante t, podendo assumir o

valor 1 ou 0 se o componente está funcionando ou não.

Cada mudança de estado de um componente ocasiona uma mudança de estado do sistema, ou seja uma transição de estado. Uma seqüência de transições define uma trajetória. A transição ocorre quando um componente que estava falho é reparado ou quando um componente funcionando falha. O comportamento do sistema é aleatório, uma vez que, a mudança de estado dos componentes também é aleatória. Então, observa-se que o estado do sistema é uma variável aleatória discreta dependente do tempo, que é assumido como variável dependente. Assim, pode-se dizer que o comportamento temporal do sistema é estocástico.

II.3.2 - Matriz de Transição

O comportamento do sistema é conhecido se a probabilidade de cada estado estar ocupado após a $(\eta+1)$-ésima transição, dada a trajetória completa ou a história de ocupação dos estados desde t_0 até t_η,

$$Pr\left\{\begin{array}{c} S(t_{\eta+1}) = i \\ S(t_\eta) = j \\ S(t_{\eta-1}) = k \\ \cdots \\ S(t_0) = m \end{array}\right\} \qquad \text{(II.5)}$$

for conhecida para todo, i, j, ..., m entre 1 e N e η igual a 0, 1, ...

A probabilidade em cada instante depende do tempo desde a inicialização (t_0) e da trajetória até o tempo considerado. O modelo markoviano só considera o último estado ocupado na determinação do comportamento futuro do sistema (sem memória). Assim, a probabilidade acima é substituida pela probabilidade de transição, ϕ_{ij}, que é definida como a probabilidade de que o sistema que ocupa o estado j ocupe o estado i após a próxima transição.

$$\phi_{ij} = Pr\left\{\begin{array}{c} S(t_{\eta+1}) = i \\ S(t_\eta) = j \end{array}\right\}, \qquad \text{(II.6)}$$

$$1 \le i, j \le N \text{ e } \eta = 0,1,2,...$$

Como ϕ_{ij} é uma probabilidade, $0 \le \phi_{ij} \le 1$, $1 \le i, j \le N$ e, como após uma

transição, obrigatoriamente um dos estados será ocupado:

$$\sum_{i=1}^{N} \phi_{ij} = 1,\ j = 1,\ 2,\ ...,\ N \qquad \text{(II.7)}$$

As probabilidades ϕ_{ij} podem ser agrupadas numa matriz de transição, Φ (Carrada e Somma, 1977):

$$\Phi = \begin{bmatrix} \phi_{11} & \phi_{12} & \cdots & \phi_{1N} \\ \phi_{21} & \phi_{22} & \cdots & \phi_{2N} \\ \cdots & \cdots & & \cdots \\ \phi_{N1} & \phi_{N2} & \cdots & \phi_{NN} \end{bmatrix},\ N = 2^n \qquad \text{(II.8)}$$

Uma matriz é dita estocástica se ela for não negativa e se a soma dos elementos de cada coluna (ou linha) for igual a 1. De acordo com a equação (II.7) a matriz (II.8) é estocástica. Outras probabilidades relacionadas com os estados ocupados pelo sistema podem ser definidas, como, por exemplo, a probabilidade do estado estar ocupado no tempo t:

$$p_i(t) = Pr\left\{ s(t) = i \right\},\ i = 1,\ 2,\ ...,\ 2^n \qquad \text{(II.9)}$$

Pode ser demonstrado (Cerqueira, 1992) que:

$$P(t+\Delta t) = \Phi(t+\Delta t, t)\ P(t) \qquad \text{(II.10)}$$

onde P(t) = [$p_i(t)$], i = 1, 2, ..., n, é o vetor de probabilidade de estado. Escrevendo a equação (II.10) para cada valor de i:

$$\begin{bmatrix} p_1(t+\Delta t) \\ p_2(t+\Delta t) \\ \cdots \\ p_n(t+\Delta t) \end{bmatrix} = \begin{bmatrix} \phi_{11}(t+\Delta t, t) & \phi_{12}(t+\Delta t, t) & \cdots & \phi_{N1}(t+\Delta t, t) \\ \phi_{22}(t+\Delta t, t) & \phi_{22}(t+\Delta t, t) & \cdots & \phi_{N2}(t+\Delta t, t) \\ \cdots & \cdots & & \cdots \\ \phi_{N1}(t+\Delta t, t) & \phi_{N2}(t+\Delta t, t) & \cdots & \phi_{NN}(t+\Delta t, t) \end{bmatrix} \begin{bmatrix} p_1(t) \\ p_2(t) \\ \cdots \\ p_N(t) \end{bmatrix} \qquad \text{(II.11)}$$

A matriz da equação (II.11) é a matriz de transição (II.8).

O conhecimento do vetor de estados P(t) para um determinado t e da matriz de transição possibilita a determinação completa do comportamento futuro do sistema.

II.3.3 - A matriz de taxas de transição

A equação básica da hipótese markoviana para sistemas cujas probabilidades de transição não dependem do tempo é:

$$\dot{P}(t) = \Lambda P(t) \qquad \textbf{(II.12)}$$

sendo $\Lambda = [\, a_{ij} \,]$, onde a_{ij} é a taxa de transição do estado i para o estado j e Λ é a matriz de taxas de transição. As taxas a_{ij} são definidas como o número de vezes que a transição ocorre a partir de um certo estado dividido pelo tempo total de permanência. Em estudos de confiabilidade são usados as taxas de falha λ e de reparo μ, como taxas de transição de estado. A taxa de falha depende das propriedades físicas do componente e das condições operacionais a que ele está submetido. A taxa de reparo depende basicamente de como o componente está disposto no sistema e quanto eficiente é a equipe de manutenção do mesmo.

Para facilitar a resolução de problemas, o sistema markoviano é representado segundo um diagrama de estados, incluindo todos os estados relevantes ocupados pelo sistema, e as possíveis transições com as taxas correspondentes.

Na Figura II.1 é exibido um exemplo de diagrama de estados para um sistema com um componente, com taxa de falhas λ e taxa de reparo μ. Para este sistema podemos representar Λ:

$$\Lambda = \begin{bmatrix} \mu & 0 \\ 0 & \lambda \end{bmatrix} \qquad \textbf{(II.13)}$$

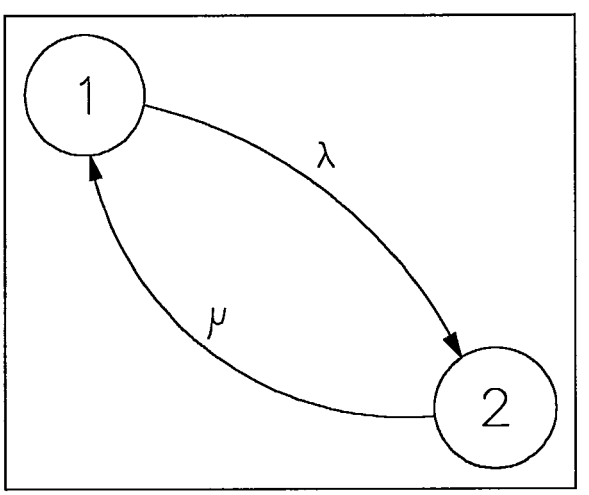


Figura II.1 - Exemplo de Diagrama de Markov

Neste caso simples, tem-se que a disponibilidade é probabilidade do sistema estar no estado 1.

II.3.4 - Solução da equação básica

Observando-se o sistema apresentado na equação (II.12), nota-se que, devido a dependência existente entre as equações do sistema, para solucioná-lo é necessário lembrar que:

$$\sum_{i=0}^{n} p_i(t) = 1 \qquad \text{(II.14)}$$

Para sistemas complexos, este tipo de problema é, normalmente, solucionado numericamente. Neste trabalho, foi utilizado um programa de computador que permite que o diagrama de estados seja desenhado graficamente e as equações diferenciais correspondentes sejam resolvidas numericamente. A partir da solução do sistema pode-se encontrar os atributos de interesse. Uma vez resolvido o sistema de equações, a indisponibilidade média no período T, pode ser calculada por:

$$\bar{A}(t) = \frac{1}{T} \int_0^T \sum_{i=1}^{N} \gamma_i \cdot p_i(t)\, dt \qquad \text{(II.15)}$$

onde o γ é um vetor cujos elementos são iguais a zero para os estados operacionais e um para os estados indisponíveis.

A freqüência esperada de acionamentos espúrios no período T pode ser encontrada por:

$$\Phi_e = \frac{1}{T} \sum_{j=1}^{N} \gamma_j \cdot \int_0^T \sum_{i=1}^{N} a_{ij} \cdot p_i(t)\, dt \qquad \text{(II.16)}$$

onde γ é um vetor cujos elementos são iguais a zero para os estados operacionais e um para os estados correspondentes a falhas espúrias.

II.4 - Avaliação de Confiabilidade por Árvores de Falhas

Outra técnica disponível, e amplamente utilizada, para a avaliação quantitativa de parâmetros de confiabilidade é a técnica de avaliação por árvores de falha (Vesely, 1981) (Oliveira, 1985) (Lees, 1980). Esta técnica é um exemplo de análise com enfoque dedutivo, e como visto anteriormente, parte da postulação da ocorrência de um determinado evento, procurando-se, em seguida, todos as formas em que as partes, do sistema em evidência, contribuem para conduzir ao referido evento. Ou seja, é efetuada uma investigação das causas de um determinado fato. Assim, a construção de uma árvore de falhas consiste em um processo lógico que, partindo-se de um evento indesejado (normalmente, falha do sistema), busca todas as combinações de falhas dos componentes que levam à ocorrência de tal evento.

A árvore de falhas é um complexo de entidades conhecidas como "portões" lógicos. Os portões simbolizam a relação booleana, ou lógica, entre eventos necessária para a ocorrência de um outro evento de nível mais alto. Combinando-se vários portões, temos que suas entradas podem ser as saídas de outros ou eventos conhecidos como "eventos básicos". Estes eventos não são combinação de nenhum conjunto de outros eventos. Desta forma, pode-se fazer uma analogia entre uma árvore de falha e um circuito elétrico booleano, onde a saída do circuito é o evento indesejado que depende das entradas, os eventos básicos, segundo uma regra lógica bem definida. Assim, pode-se dizer que, como primeiro resultado da análise por árvores de falhas obtem-se um diagrama lógico. Na Figura II.2 é mostrada um exemplo de árvore de falhas para um sistema simples.

Após a construção da árvore de falhas, pode-se representá-la através de uma expressão booleana. Esta expressão pode ser reduzida, ou otimizada, e dela pode-se determinar todos os cortes mínimos associados à árvore. Estes cortes mínimos definem os modos de falha do evento topo. Uma definição formal de corte mínimo é a seguinte: um corte mínimo é a menor combinação de falhas de componentes que, se ocorrerem todas, implicam na ocorrência do evento topo. Pela definição, um corte mínimo é aquela combinação de eventos básicos suficientes para estabelecer a ocorrência do evento topo, sendo que esta combinação é sempre a menor possível, ou seja, se qualquer um dos eventos básicos, desta mesma combinação, não ocorrer, o evento topo não ocorrerá. A relação dos cortes mínimos é um resultado qualitativo que mostra ao

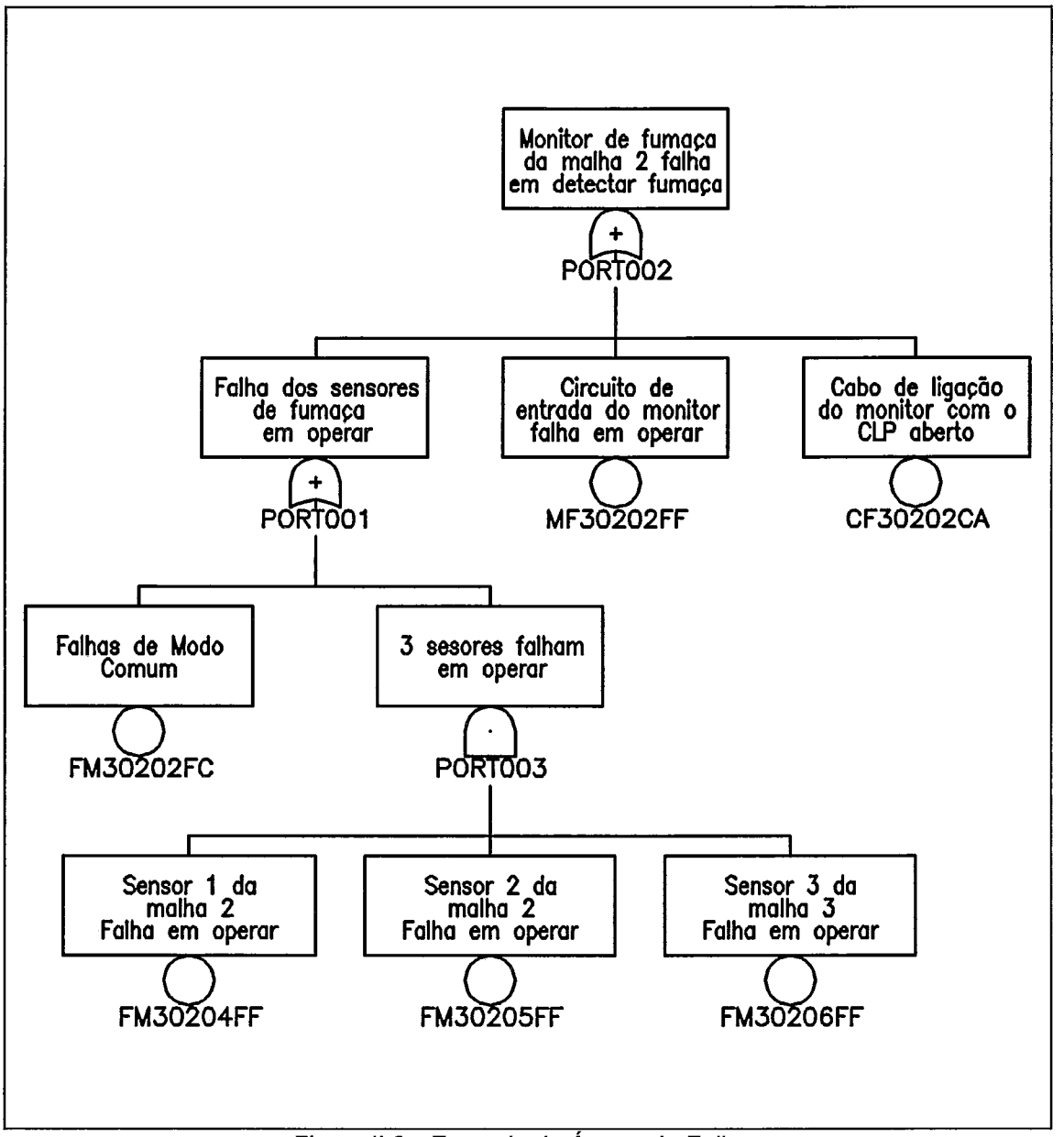


Figura II.2 - Exemplo de Árvore de Falhas

analista o conjunto de falhas capazes de levar ao evento topo. Por exemplo, a expressão booleana resultante da árvore mostrada na Figura II.2 é:

$$PORT002 = MF30202FF + MF30202CA + FM30202FC + FM30204FF \cdot FM30205FF \cdot FM30206FF,$$

onde o simbolo "+" significa a operação lógica "OU" e o simbolo "·" a operação "E". Desta expressão pode-se diretamente, sem simplificação alguma, obter-se os cortes mínimos mostrados na Tabela II.1, mostrada abaixo:

Tabela II.1 - Cortes Mínimos para a Árvore Exemplo

Corte	Ordem
MF30202FF	1
MF30202CA	1
FM30202FC	1
FM30204FF, FM30205FF, FM30206FF	3

Uma árvore de falhas consiste em um conjunto finito de cortes mínimos, que são únicos para aquele evento topo. A ordem do corte reflete o número de eventos contidos nele. Por exemplo, um evento que é capaz de provocar sozinho o evento topo é um corte mínimo de primeira ordem.

Os resultados quantitativos que podem ser avaliados após a determinação dos cortes mínimos são: as probabilidades, ou freqüência, de ocorrência de cada um dos corte mínimos; a importância de cada corte mínimo; e a probabilidade de ocorrência do evento topo. De forma seqüencial, primeiro avalia-se a probabilidade (ou freqüência) dos eventos básicos (a partir dos dados de falhas dos componentes que ele representa); em seguida, a probabilidade associada aos cortes mínimos e, por último, a do evento topo. A importância de cada corte mínimo também é obtida desta mesma maneira.

A avaliação quantitativa de árvores de médio e grande porte é, geralmente, efetuada por intermédio de programas de cálculo especialmente desenvolvidos para isto. Alguns programas, como o utilizado neste trabalho, podem ser sofisticados a ponto das árvores poderem ser desenhadas e quantificadas totalmente no computador(Albuquerque, Gamal e Pinto, 1992).

Assim, de uma maneira geral, as etapas de realização de uma análise por árvore de falhas são as seguintes:

1) definição do sistema;
2) formulação dos eventos topo;
3) construção da árvore;
4) levantamento dos dados de falha dos eventos básicos;
5) determinação dos cortes mínimos;
6) avaliação quantitativa;
7) identificação dos cortes mínimos mais importantes;

8) conclusões e recomendações.

II.5 - Análise Custo-Benefício

A análise custo-benefício consiste no levantamento dos custos e benefícios resultantes da implementação de uma dada configuração. O balanço econômico destes custos e benefícios indicará se a mesma é recomendável ou não: se positivo, indica que haverá um ganho líquido anual (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 apresentaram as melhores relações de benefício-custo.

Os custos associados às configurações são relacionados à implementação dos equipamentos e à manutenção destes. Por sua vez, o benefício resultante da implementação de uma configuração é obtido computando-se: a redução das perdas esperadas devido a acidentes (benefício resultante da atuação do sistema de proteção, evitando o acidente), e a redução dos ganhos esperados devido a falhas espúrias (redução da freqüência de falhas espúrias do sistema de detecção de incêndio).

Os detalhes da avaliação dos custos e benefícios estão apresentados abaixo.

II.5.1 - Avaliação do Custo

A avaliação do custo de cada configuração é feita computando-se os custos de implementação da mesma, os quais são representados pela soma:

- dos custos de capital da implementação;
- dos custos de instalação; e
- dos custos de manutenção dos equipamentos.

Para fins de comparação, os custos totais de cada configuração são apresentados de forma anualizada. Para tanto, leva-se em consideração o

período de vida útil da modificação e uma taxa de juros, que reflete o custo de capital de mercado. O valor anualizado corresponde a um certo valor presente pode ser calculado pela conhecida equação:

$$V_a = \frac{i \cdot Vp}{1-\left(\frac{i}{1+i}\right)^n} \qquad \textbf{(II.17)}$$

onde:

V_a = valor anualizado (dólares/ano);

i = taxa de juros anual;

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

V_p = valor presente (dólares).

II.5.2 - Avaliação do Benefício Esperado

O benefício esperado com a configuração pode ser dividido em duas parcelas:

1) a redução das perdas esperadas devido a acidentes (perdas econômicas + valor monetário das perdas humanas); e

2) a redução dos ganhos devido a introdução falhas espúrias causadas pelo sistema de proteção.

Assim o benefício esperado para uma configuração é dado por:

$$B_{Conf} = R_{pe} - R_{pfe} \qquad \textbf{(II.18)}$$

onde:

B_{Conf} = benefício esperado;

R_{pe} = redução das perdas esperadas devido a acidentes; e

R_{pfe} = perdas devido a ocorrência de falhas espúrias.

A redução das perdas esperadas devido a acidentes para uma dada configuração é calculada com base indisponibilidade da mesma, na freqüência anual de acidentes e no custo da perda média de um acidente, pela fórmula:

$$R_{pe} = F_{ac} \cdot C_{ac} \cdot (1 - \bar{A}_{sis}) \qquad \textbf{(II.19)}$$

onde:

F_{ac} = freqüência média de ocorrência de acidentes;

C_{ac} = perda média esperada por acidente; e

$\bar{A}_{sis}$ = Indisponibilidade do sistema de proteção.

Apesar da introdução do sistema, persistirá ainda uma perda esperada residual devido a probabilidade de falhas do sistema (indisponibilidade). Esta perda esperada residual pode ser calculada por:

$$P_{esp} = F_{ac} \cdot C_{ac} \cdot \bar{A}_{sis} \qquad \textbf{(II.20)}$$

As reduções do benefício devido a falhas espúrias são calculadas através do produto da freqüência de falhas espúrias, de uma dada configuração, pelo custo de uma falha espúria.

III. ARQUITETURAS DE CLPs UTILIZADAS EM SISTEMAS DE PROTEÇÃO

III.1 - Introdução

Criados para substituir os controles eletro-mecânicos utilizados na indústria automotiva, os Controladores Lógicos Programáveis (CLP) vêm, desde sua criação, sendo largamente empregados no controle de processos industriais. Com o passar dos anos, esses equipamentos vêm ganhando complexidade para poderem operar, com velocidade e precisão, nas mais sofisticadas tarefas de controle e automação.

As características programáveis do CLP valorizam o seu uso em processos que estão em contínuo estado de modificação e evolução. Alguns controladores mais sofisticados possuem larga capacidade de armazenamento de dados, podem ser ligados em rêde e ainda serem programados a distancia.

Em decorrência das responsabilidades cada vez maiores, colocadas sobre este tipo de equipamento, as preocupações com seus níveis de confiabilidade tem sido cada vez maiores (Fisher e Thomas, 1990). Assim sendo, os fabricantes têm se concentrado em fornecer aos usuários alternativas de configurações tolerantes a falha. Algumas soluções de engenharia encontradas criaram esquemas de sofisticados diagnósticos internos, de vários elementos do equipamento, que conduzem o sistema a uma condição segura no momento da detecção de falhas internas. Por intermédio destes mesmos diagnósticos, esquemas redundantes podem ser projetados.

Embora os meios de detecção de falhas internas estejam cada vez mais sofisticados, existe ainda um conjunto de falhas que não são possíveis de serem detectadas, passando, perante aos circuitos e rotinas de diagnósticos, como situações de operação normal. Estas falhas somente podem ser detectadas mediante a um teste total do sistema. O teste é efetuado simulando uma determinada situação que o sistema normalmente responderia se estivesse em perfeitas condições.

De uma forma geral, um Controlador Lógico Programável é constituído de quatro elementos principais:

- o processador (CPU);

- os equipamentos de entrada/saída;

- a fonte de potência;

- o terminal de programação.

Tendo em vista que a função do terminal de programação consiste unicamente em possibilitar a colocação das instruções de controle no processador, este elemento não será analisado neste trabalho. Como a arquitetura do equipamento pode variar muito de um fabricante para outro, escolhemos neste trabalho, os equipamentos produzidos pela "**RELIANCE**", um fabricante norte-americano de controladores programáveis utilizados na indústria automobilística e plataformas de petróleo. Será mostrada a seguir uma breve descrição dos equipamentos empregados e das configurações utilizadas neste trabalho.

III.2 - Descrição dos Equipamentos

O CLP escolhido é um controlador lógico programável com capacidade de endereçar até 8192 pontos de entrada e saída digitais. A unidade central de processamento, implementada usando o microprocessador de 16 bits Motorola 68000, fornece ao usuário uma memória disponível para aplicação de até 104 K palavras de 16 bits.

O controlador pode ser dividido em dois subsistemas distintos ligados entre sí. São eles:

- **Unidade de Processamento** e
- **Sistema de Entrada e Saída**.

A **Unidade de Processamento** é responsável pela execução das operações lógicas e de controle do sistema. O **Sistema de Entrada e Saída** serve de interface entre o mundo real e a **Unidade de Processamento**. O **Sistema de Entrada e Saída** pode ser ligado à **Unidade de Processamento** de duas formas básicas:

- diretamente, com o uso de canais dedicados que existem na placa do **processador** ou canais dos **processadores de entrada e saída remoto**;
- por intermédio de uma rede local.

Segue agora, uma descrição mais detalhada dos dois subsistemas.

III.2.1 - A Unidade de Processamento

A **Unidade de Processamento** é formada por diversas partes (placas) que se comunicam entre sí através de dois barramentos. São eles : o **barramento local**, que permite a expansão da capacidade de memória do sistema; e o **Multibus**, que possibilita a conexão de mais de um processador (para aplicações que exijam processamento paralelo), interfaces de E/S remotas e interfaces de E/S inteligentes.

As partes usadas na composição da **Unidade de Processamento** são :

- **"Rack" de Cartões** - Onde são montados os componentes do sistema. Na parte posterior do "rack" estão localizados os barramentos do sistema ("back plane" - formado pelo **Multibus** e barramento local). O **"rack"** montado pode operar sozinho, como um sistema independente, ou como um subsistema remoto de E/S;

- **Fonte de alimentação** - Fornece todas as tensões necessárias para manter em funcionamento os circuitos do sistema ligados ao "rack". Fornece, também, como será visto mais tarde, a alimentação dos trilhos ligados diretamente ao **"Rack" de Cartões**. Posicionada na fonte de alimentação existe um relé, cujos contados estão disponíveis ao projetista, que é acionado pelos circuitos de diagnóstico da CPU, toda vez que for detectada uma falha na mesma. Este relé é conhecido como "**Relé de Pronto**";

- **Unidade de Processamento CPU** - Exerce o controle do sistema e faz a verificação dos erros através de diagnósticos internos e pela ação de um "Watch Dog Timer". Executa as ações de controle pro-

gramadas pelo usuário. O programa é introduzido por meio de um terminal especial de programação e é expresso na forma de diagramas "ladder" e diagramas "ladder" estendidos. Para armazenar o programa de controle, esta CPU provê, internamente, 8K palavras de 16 bits de memória interna não volátil, que pode ser expandida até 104K palavras com o uso de placas adicionais. Fisicamente o processador é formado por duas placas. Uma corresponde ao **processador lógico** que é responsável pela execução das instruções "ladder" e atuação sobre as E/S ligadas diretamente a ele. Quatro portas de comunicação presentes na fronte do **processador lógico** fazem a interface com os **Dispositivos de E/S** (**Trilhos de E/S** ou **Cabeças Locais**, como será visto mais adiante) usando um protocolo serial a uma taxa de 300 Kbauds com verificação de paridade. A outra placa corresponde ao **processador de controle** que atua diretamente sobre os demais periféricos ligados no "rack".;

- **Processador de E/S local** - havendo necessidade de ligar mais **Dispositivos de E/S**, além daqueles ligados ao **processador lógico**, este processador pode ser empregado. Assim, mais 4 portas de comunicação serão adicionadas ao sistema. Estas portas tem características semelhantes às existentes na fronte do **processador lógico**;

- **Processador de E/S remoto** - Este processador é usado para fazer a ligação entre unidades remotas do sistema. Ele pode concentrar os dados provenientes de até 32 subsistemas remotos e enviá-los, via **Multibus**, ao processador da **CPU**. O protocolo de comunicação é serial, a uma taxa de 800 Kbauds e é totalmente implementado por um processador Motorola 68000 interno, liberando o processador central da verificação de erros de comunicação entre os subsistemas e o **processador remoto**. A distância máxima entre o **processador de E/S remoto** e o subsistema remoto é de 3600 metros. Este processador pode servir de processador escravo em "racks" desprovidos de **Unidade Central de Processamento** (esses "racks" servem como um subsistema de E/S remotos);

- **Dispositivos E/S Numéricos e dispositivos de E/S inteligentes** -

Estes dispositivos, ligados ao processador via **Multibus**, permitem acesso a dados numéricos com alta velocidade. Esses dados podem ser provenientes de sensores de pressão, temperatura, velocidade, etc. Os dispositivos inteligentes tem capacidade de processamento próprio e liberam a **CPU** de algumas tarefas de controle.

III.2.2 - Sistema de Entrada e Saída

As unidades de entrada e saída são organizadas de forma modular, permitindo o seu dimensionamento de acordo com as necessidades do usuário. Três componentes básicos compõem o sistema, são eles :

- **Trilho de Entrada e Saída** - Serve de elemento de conexão entre as variáveis do campo e os **módulos de Entrada e Saídas**. Acondiciona fisicamente até 8 **Módulos de E/S**, podendo assim, fornecer até 16 pontos de entrada ou saída;

- **Módulos de Entrada e saída** - São os elementos de interface entre os equipamentos do campo e a **CPU**. Existe uma variedade de módulos escolhidos de acordo com o tipo de variável a ser monitorada, ou tipo atuação a ser efetuada. Cada módulo possui dois canais de entrada ou dois canais de saída disponíveis;

- **Interface de Entrada e Saída** - Esta parte do sistema faz a conexão física entre a **CPU** e os **Trilhos de E/S**. Esta interface pode ser estabelecida de 3 formas distintas, são elas:

    - **Diretamente** - Desta forma o **trilho** é ligado a uma das 4 portas de comunicação presentes no fronte do **CPU** ou **Processador de E/S local**. Assim, tem-se até 16 E/S por **trilho**. A alimentação do **trilho** é fornecida pela fonte que alimenta o **"rack"** onde está montado a **CPU**;

    - Usando uma **Cabeça Local** - Este dispositivo é um multiplexador que permite conectar qualquer uma das portas de comunicação do fronte da **CPU** (ou **Processador de E/S**

local) com 4 trilhos, aumentando, assim, a capacidade de uma porta de 16 para 64 entradas de E/S. A **Cabeça Local** possui uma fonte de alimentação própria que alimenta os **trilhos** ligados a ela;

- Usando uma **Cabeça Remota** - Este dispositivo é usado como alternativa na formação de subsistemas remotos. Ligada ao **Processador de E/S remoto** através de um cabo coaxial, a **Cabeça Remota** possui 4 portas de comunicação (idênticas às existentes na **CPU**) que podem ser ligadas a **trilhos** ou **Cabeças Locais**. Uma fonte de alimentação própria pode alimentar até quatro **trilhos** ligados a ela.

III.3 - Arquiteturas Redundantes de CLPs

Devido o pouco conhecimento dos modos de falha dos CLPs, houve uma rejeição inicial ao uso dos mesmos em aplicações críticas, como os sistemas de proteção e intertravamento. Uma das maiores dificuldades dos projetistas era a de garantir uma caraterística "fail-safe" aos sistemas usando CLPs. O acúmulo de experiência operacional decorrente do uso industrial crescente, bem como o contínuo aperfeiçoamento dos controladores, permitiram a obtenção de sistemas tecnologicamente mais evoluídos. Aliado a esses fatos, a concepção de sistemas com CLPs redundantes, tornaram estes equipamentos uma opção cada vez mais atraente aos projetos de sistemas de segurança e intertravamento.

Além dos procedimentos normais, que garantem a qualidade de um projeto eletrônico, como escolha de bons componentes, uso de circuitos bem dimensionados e etc, o projeto tolerante a falhas dispõe de ferramentas importantes, como: diagnóstico de falhas e redundância. A partir de um diagnóstico de erro, indicando a presença de uma disfunção de uma determinada parte do equipamento, o sistema é capaz de substituir esta parte, colocando em funcionamento uma outra que estava em "stand-by". Esta operação permite que o equipamento avariado, possa ser consertado, sem que todo o sistema seja desligado. Para aquele conjunto de falhas que não podem ser detectadas, ou seja, nenhum diagnóstico de falha conclusivo pode ser gerado pelo sistema. Emprega-se uma técnica de votação entre vários subsistemas redundantes ligados

em paralelo. Por exemplo: um determinado sensor pode ser ligado a dois, ou mais, cartões de entrada ao mesmo tempo. O sistema deverá avaliar, mediante os resultados apresentados pelos cartões qual o "status" real da variável que está sendo monitorada pelo sensor.

Com o emprego das técnicas descritas acima, serão formadas as configurações analisados neste trabalho, ou seja:

- Configuração **Simplex**: Sem qualquer tipo de redundância, *simplesmente servirá como base de comparações;*

- Configuração **Dual-Simplex**: Nesta configuração é usado um mecanismo de redundância com duas CPUs, que são capazes de controlar um conjunto de equipamentos de entrada e saída comum. Uma controla realmente o sistema, enquanto a outra monitora o funcionamento correto da primeira. Na ocorrência de uma falha a segunda assume o controle, enquanto a CPU avariada é reparada;

- Configuração **Dual-Dual**: Dois conjuntos completos, CPU, entradas e saídas, idênticos, são colocados em funcionamento ao mesmo tempo. As saídas de cada subsistema são votadas por mecanismo de relés eletro-mecânicos;

- Configuração **Triplex**: De forma semelhante a configuração Dual-Dual, são colocados três sistemas completos, que são votados na saída.

Descrições mais detalhadas de cada configuração serão mostradas a seguir.

III.2 - Configuração Simplex

A configuração **SIMPLEX** é caracterizada pelo uso de apenas um único CLP ligado aos dispositivos de entrada e saída. Nesta configuração não há nenhum tipo de redundância. A Figura III.1 mostra um diagrama simplificado da arquitetura básica deste tipo de configuração.

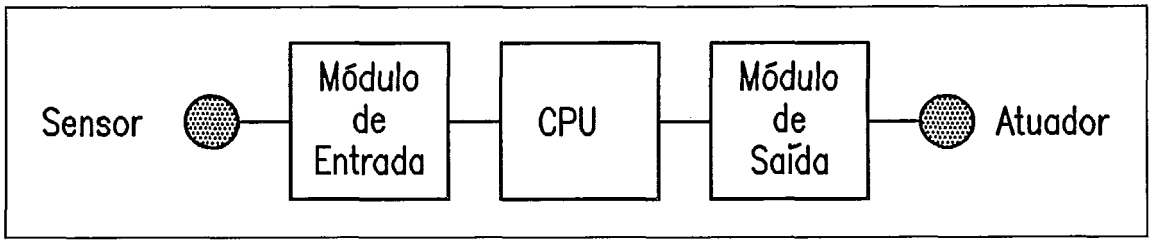


Figura III.1 - Arquitetura Básica da Configuração **SIMPLEX**

Para a análise da configuração SIMPLEX será adotada a estrutura representada na Figura III.2. Os componentes usados nesta composição são:

- Uma **CPU**;
- Uma **Fonte de alimentação** para o "**Rack**" da CPU;
- Uma **Interface de E/S Remota**;
- Uma **Cabeça Remota**;
- Uma **Cabeça Local**;
- Um **Trilho de E/S**;
- Dois **Módulos de E/S** (um como entrada, outro como unidade de saída).

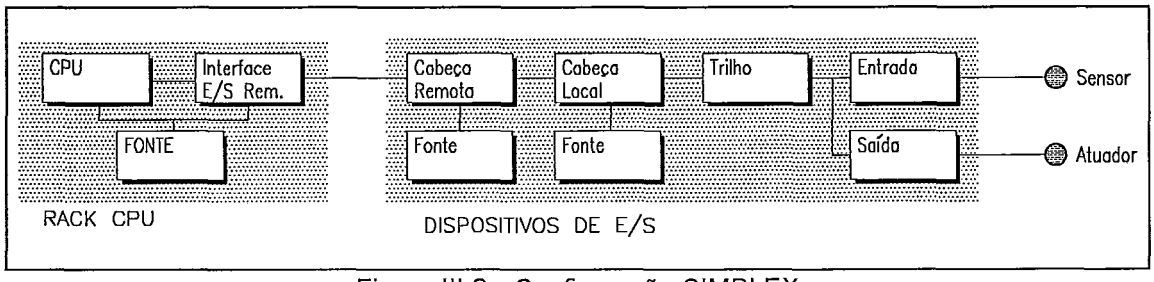


Figura III.2 - Configuração SIMPLEX

Acompanhando a Figura III.2 pode-se notar que, uma **Cabeça Local** é ligada a uma **Cabeça Remota** que se comunica com a **CPU** por intermédio de uma **Interface de E/S Remota**. Um **trilho**, conectado a dois **Módulos de E/S** e à **Cabeça Local**, serve de dispositivo de entrada e saída. A fonte de alimentação do "rack" alimenta a CPU. Os dois cartões de E/S estão ligados ao mesmo **trilho**, portanto estão alimentados pela fonte da **Cabeça Local**. A **Cabeça Remota** tem uma **Fonte de Alimentação** própria.

Para análise desta configuração os cartões de entrada e de saída foram ligados ao mesmo conjunto de "Cabeça Remota"-"Cabeça Local"-"Trilho", para que fosse obtida a configuração de maior confiabilidade, isto é, com menos componentes em série.

III.3 - Configuração Dual-Simplex

A configuração Dual-Simplex é caracterizada pela duplicação das Unidades de Processamento (CPUs), dispostas em uma arquitetura que permita o compartilhamento das Unidades de Entrada e Saída. Uma CPU é mantida **ativa** e controla o sistema, a outra servirá de unidade "**backup**" em caso de falha da unidade **ativa**. Na Figura III.3 é mostrado um diagrama simplificado desta configuração.

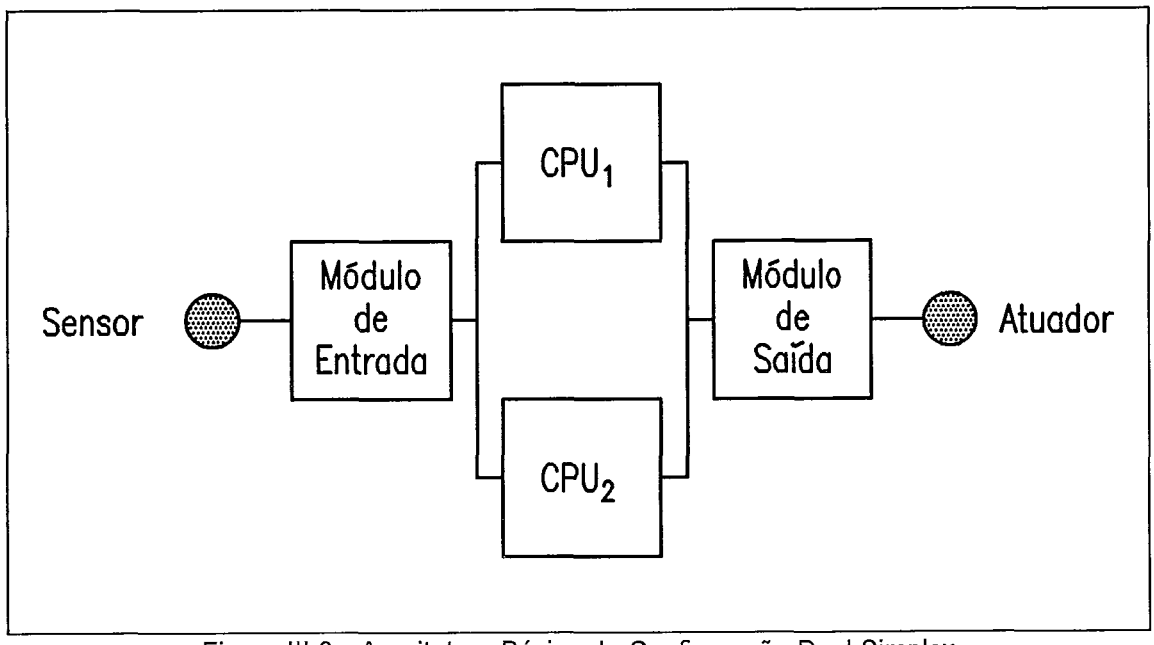


Figura III.3 - Arquitetura Básica da Configuração Dual-Simplex

Para a análise da configuração Dual-Simplex serão utilizados os seguintes componentes:

- Dois "**racks**" contendo cada um :
  - Uma **CPU**;
  - Uma **Fonte de Alimentação**;
  - Uma **Interface de E/S Remota**;
  - Um cartão **RDX**;
  - Um **Trilho de E/S**;
  - Dois **cartões de Entrada**;
  - Um **cartão de Saída**;
- Dispositivos de Entrada e Saída compostos por :

- Uma **Cabeça Remota**;
- Uma **Cabeça Local**;
- Um **Trilho de E/S**;
- Um **Cartão de Entrada**;
- Um **Cartão de Saída**.

Na Figura III.4 é mostrada a arquitetura adotada para a configuração Dual-Simplex. Dos dispositivos descritos acima, somente o cartão **RDX** não foi descrito anteriormente. Este cartão é basicamente um dispositivo de comunicação de dados de alta velocidade. O **RDX** é capaz de detectar erros de comunicação e erros de "**hardware**" internos.

Como pode ser acompanhado na Figura III.4, os dispositivos de entrada e saída são ligados aos processadores por intermédio de processadores remotos. Um "**rack**", dito **Ativo** é responsável pelo controle do sistema. A outra unidade, dita "**Stand by**", monitora através do trilho ligado diretamente à porta 0 da CPU, o **relé de pronto** do "**rack**" ativo. Quando na falha da unidade **ativa** este relé será desativado. Como a unidade em "**Stand By**", não está nem adquirindo dados ou controlando o sistema, torna-se necessário que o contexto de controle seja transferido de tempos em tempos da unidade **ativa** para a unidade "**Stand By**". Para tal intento o cartão **RDX** é utilizado. A cada varredura do sistema as variáveis de estado são enviadas da unidade **ativa** para a "**Stand By**". Desta forma, na ocorrência de alguma falha, a **CPU** "**backup**" assumirá o controle do sistema e usará as variáveis de estado da última transferência efetuada.

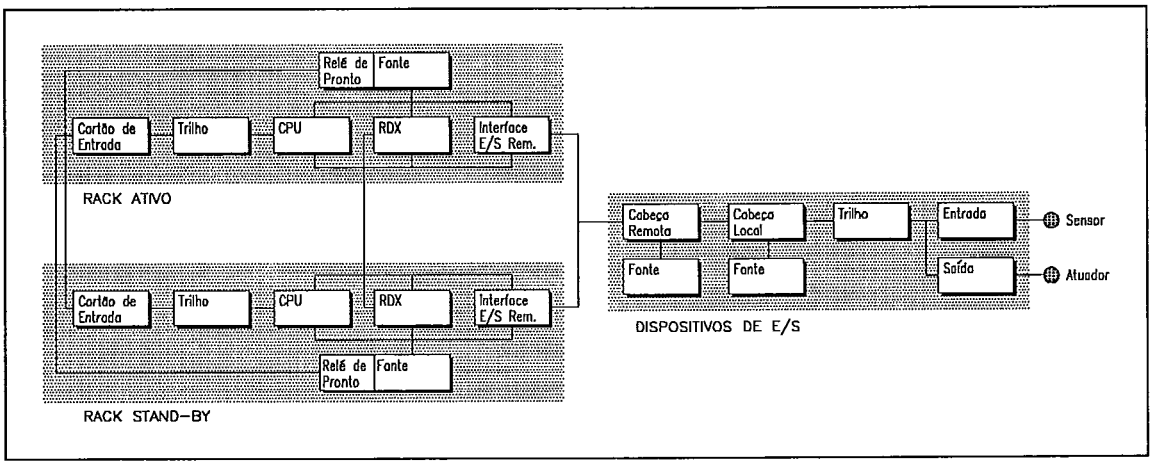


Figura III.4 - Configuração Dual-Simplex

Uma unidade de saída, conectada ao trilho ligado diretamente à **CPU**, é utilizada para estabelecimento de uma indicação visual que mostra qual

a unidade ativa do sistema. Uma outra unidade de entrada serve para ligação de uma chave de seleção de unidade ativa, que é usada para desativar a **CPU** ativa, de forma a colocá-la em manutenção preventiva.

III.4 - Configuração Dual-Dual

A configuração Dual-Dual é caracterizada pela duplicação das Unidades de Processamento (CPUs) e duplicação dos dispositivos de Entrada e Saída. Esta configuração, mostrada na Figura III.5, é um sistema redundante onde as duas unidades trabalham em paralelo, ou seja, estão igualmente ativas no controle do processo. Entretanto, os módulos de saída são ligados a um votador composto por relés eletro-mecânicos.

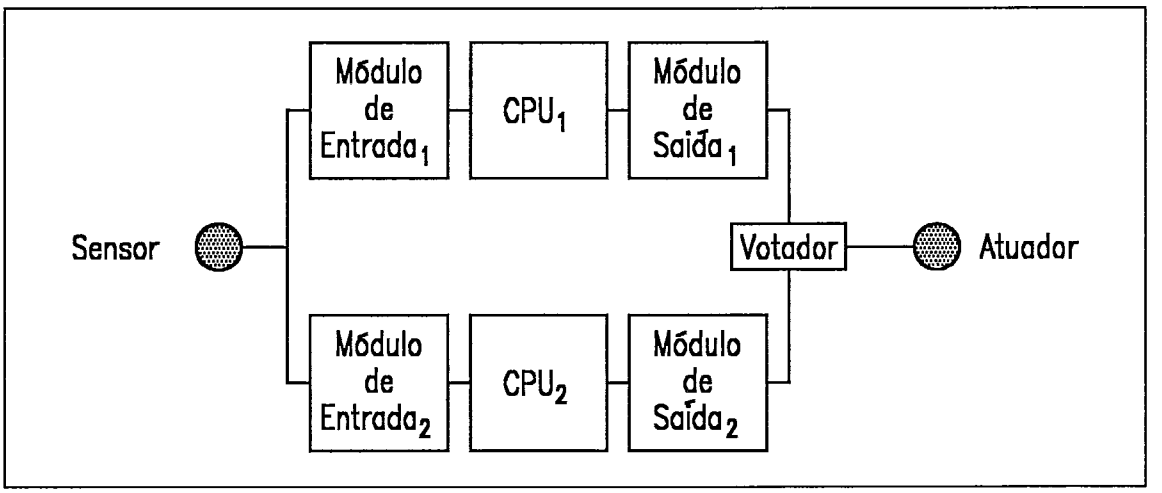


Figura III.5 - Arquitetura Básica da Configuração Dual-Dual

Neste caso específico, dois tipos de votação são possíveis:

- Votação **1-de-2** para acionar - Para acionamento do sistema de proteção, é necessário que apenas um das duas unidades tome a decisão de acionamento;

- Votação **2-de-2** - O acionamento do sistema de proteção só é efetuado quando as duas unidades tomam a decisão de acionamento conjuntamente.

Os diagramas dos votadores, citados acima, são implementados utilizando-se relés eletro-mecânicos e são mostrados na Figura III.6. Em ambos os casos são

utilizados dois relés. Os circuitos se comportam como portões lógicos do tipo "E", para o caso do votador 1-de-2 e "OU" para o outro caso. Para o perfeito entendimento do circuito, é conveniente lembrar que o CLP aciona o sistema de proteção enviando um sinal "0" para a sua saída (ou seja, lógica negativa). Isto é feito de forma que uma possível queda de alimentação do sistema de monitoração cause um acionamento do sistema de proteção (preservando a caraterística "fail-safe" do sistema). Assume-se que o desligamento espúrio em qualquer um dos subsistemas é sempre detectado. Neste trabalho, a configuração dual-dual será analisada para os dois tipos de votação citados acima.

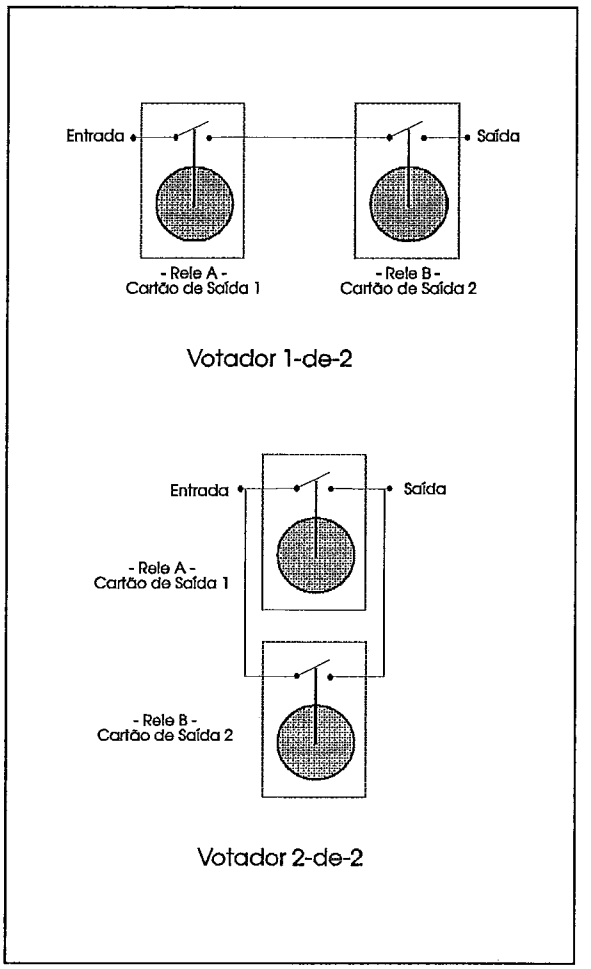


Figura III.6 - Tipos de Votadores para Configuração Dual-Dual

Para análise, o sistema foi subdividido em dois subsistemas básicos (ou canais) ligados ao dispositivo votador, verificando-se o efeito de cada condição de falha (**falha crítica**, **desligamento espúrio**) dos subsistemas sobre o sistema como um todo. Para a análise dos efeitos das falhas do dispositivo votador, este é dividido em seus componentes, ou seja os relés, de forma que o efeito da falha de cada um deles possa ser associado a uma falha nos cartões de saída.

Na configuração da configuração dual-dual, analisada, serão utilizados os seguintes componentes:

- Dois "**racks**" contendo cada um :
  - Uma **CPU**;
  - Uma **Fonte de Alimentação**;
  - Uma **Interface de E/S Remota**;

- Dois "**racks**" de Entrada e Saída compostos por :
  - Uma **Cabeça Remota**;
  - Uma **Cabeça Local**;
  - Um **Trilho de E/S**;
  - Um **Cartão de Entrada**;
  - Um **Cartão de Saída**.

- Um votador composto por relés.

Na Figura III.7, é mostrada a arquitetura adotada para a configuração do Dual-Dual. Como pode ser acompanhado na mesma figura, os dispositivos de entrada e saída são ligados aos processadores por intermédio de processadores remotos. Os módulos de saída são ligados ao votador.

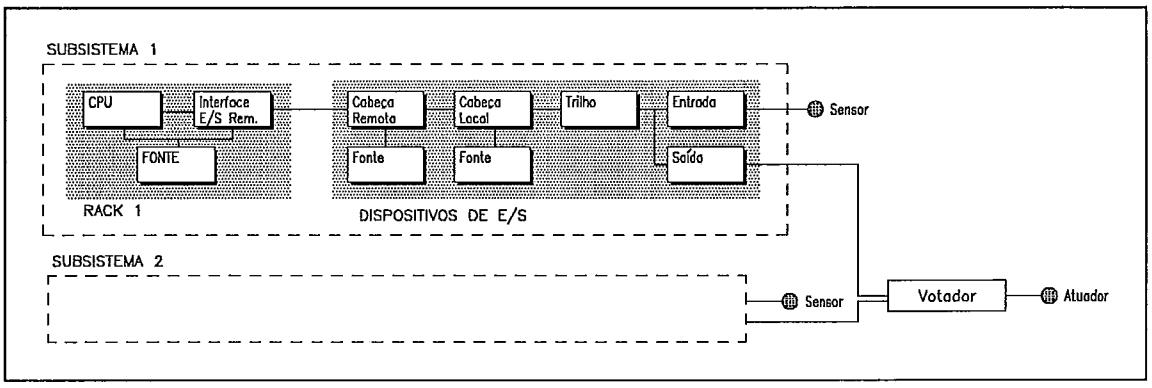


Figura III.7 - Configuração Dual-Dual

III.5 - Configuração Triplex

A configuração **TRIPLEX** é caracterizada pelo uso de três sistemas de controle completos (dispositivos de entrada, CPU e dispositivos de saída) colocados em paralelo. De forma semelhante a configuração **DUAL-DUAL** as saídas de cada sistema são ligadas a um sistema de votação composto por relés eletro-mecânicos. A votação escolhida para este trabalho foi a 2-de-3 (Finkel e Kirchoff, 1985). Assim sendo, os três sistemas estão totalmente isolados um do outro, permitindo a manutenção de cada sistema em separado. Na Figura III.8 é mostrada um diagrama simplificado desta configuração.

O diagrama do votador 2-de-3 implementado por relés é mostrado na Figura III.9. Para cada saída é usado um relé com três contatos cada um. Dois contatos são usados para implementar a lógica do votador 2-de-3. O terceiro serve para monitorar o correto funcionamento do relé, e deve ser

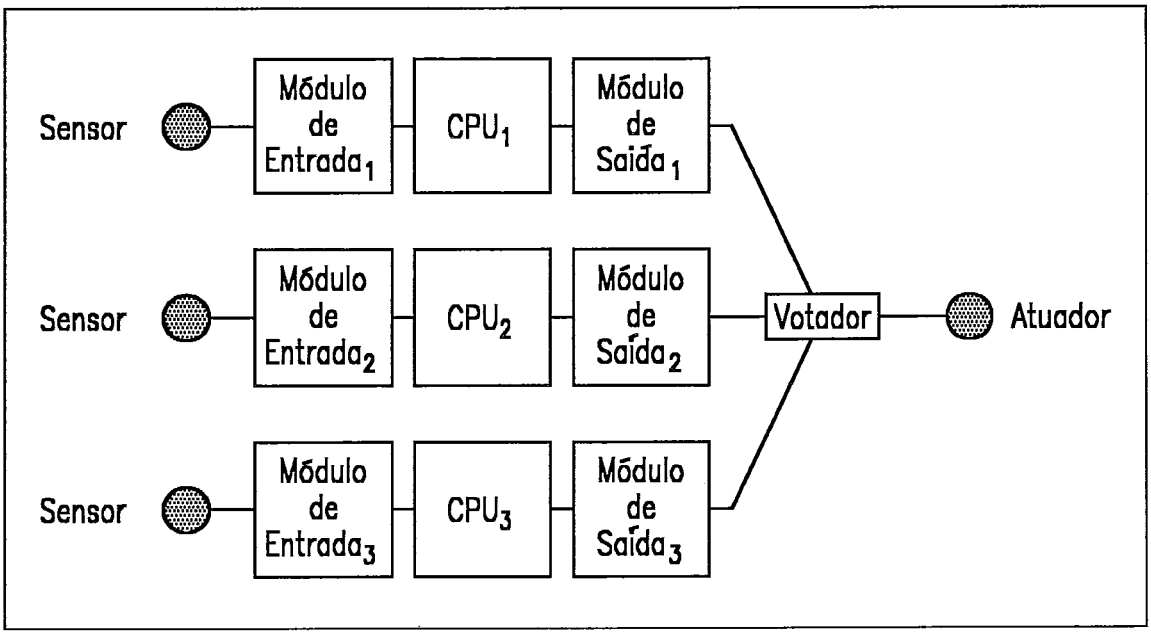


Figura III.8 - Arquitetura Básica da Configuração TRIPLEX

conectado a um cartão de entrada do CLP que o controla. O circuito funciona de maneira simples: o barramento mostrado na Figura é composto por três linhas de alimentação. Estas linhas são responsáveis pela alimentação dos módulos de saída dos CLPs, e para que esta mesma alimentação chegue a estes módulos é necessário que, pelo menos uma das linhas do barramento não esteja interrompida (na condição normal de funcionamento as três linhas estão conduzindo). Os relés são colocados de forma que quando dois deles abrem, as três linhas são interrompidas simultaneamente.

O sistema foi subdividido em três subsistemas básicos (ou canais), ligados ao dispositivo votador. A análise desta configuração foi feita analisando-se o efeito de cada condição de falha (**falha crítica**, **desligamento espúrio**) dos subsistemas sobre o sistema como um todo. Para a análise dos efeitos das falhas do dispositivo votador, este foi dividido em seus componentes (relés), de forma que o efeito da falha de cada um dos relés pode ser associado a uma falha nos dispositivos de saída do controlador que o aciona.

O efeito de um desligamento espúrio em qualquer um dos subsistemas é sempre detectado, e que o efeito da falha detectada em dois subsistemas, causa um desligamento espúrio.

Para a análise da configuração triplex serão utilizados os seguintes componentes:

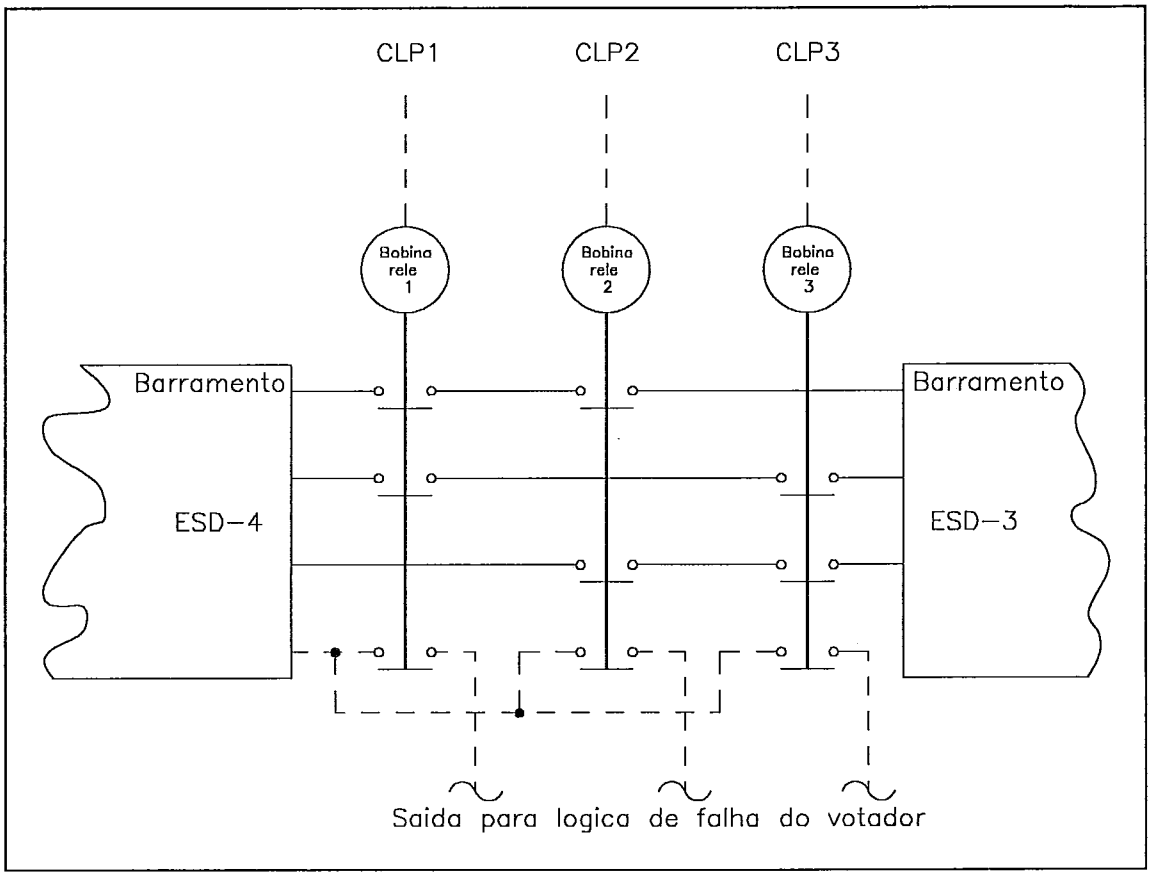


Figura III.9 - Diagrama do Votador 2-de-3

- Três "**racks**" contendo cada um :
  - Uma **CPU**;
  - Uma **Fonte de Alimentação**;
  - Uma **Interface de E/S Remota**;

- Três "**racks**" de Entrada e Saída compostos por :
  - Uma **Cabeça Remota**;
  - Uma **Cabeça Local**;
  - Um **Trilho de E/S**;
  - Um **Cartão de Entrada**;
  - Um **Cartão de Saída**.

- Um votador 2-de-3 composto por relés.

Na Figura III.10, é mostrada a arquitetura adotada para a configuração do **TRIPLEX**. Como pode ser acompanhado na mesma figura, os dispositivos de entrada e saída são ligados aos processadores por intermédio de processadores remotos. Os módulos de saída são ligados ao votador.

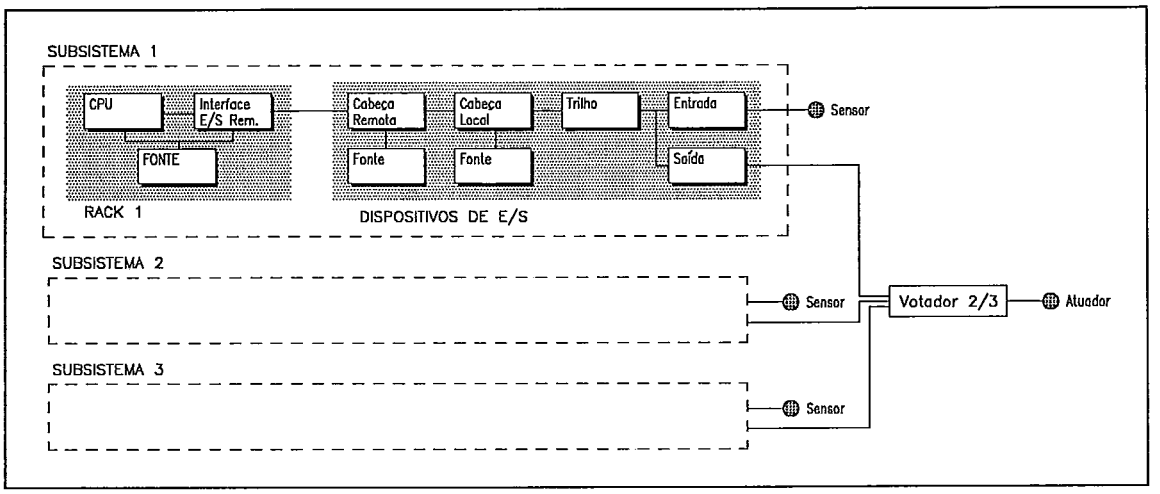


Figura III.10 - Configuração TRIPLEX

IV. MODELAGEM DO PROBLEMA E RESULTADOS OBTIDOS

IV.1 - Introdução

Neste Capítulo serão apresentados os modelos de cálculo usados para modelar as configurações de CLPs e o caso exemplo. Cada uma das configurações de CLP foi modelada utilizando-se um modelo markoviano. Para a avaliação de custo benefício, foi necessária a modelagem de uma aplicação de segurança, onde os próprios são empregados. O exemplo escolhido é a malha de detecção de incêndio de uma zona de produção de uma plataforma de petróleo. Este sistema foi modelado por intermédio de árvores de falhas. No final deste capítulo, será exibido o resultado final da análise de custo-benefício.

IV.2 - Modelagem das Configurações

Foi adotada a modelagem markoviana para a avaliação da confiabilidade das configurações de CLP. Esta modelagem permite que sistemas com componentes reparáveis possam ser modelados com bastante precisão. A título de ilustração será apresentada, neste capítulo, o exemplo da modelagem da configuração TRIPLEX 2-de-3. A modelagem das demais configurações podem ser obtidas nos trabalhos de Oliveira e Gamal (1991) e Francisco (1992).

Os modos de falha de cada componente e os respectivos efeitos sobre os subsistemas (expressos em termos da condição de falha resultante em cada canal) estão indicados na Tabela IV.1.

As condições de **"componente em curto"** e **"componente em aberto"** indicam, respectivamente, a presença de um sinal lógico "1" ou um "0" no componente. A hipótese adotada neste trabalho é que as saídas do sistema de segurança, ou intertravamento, são mantidas normalmente energizadas (presença do sinal lógico "1") e que, portanto, o sistema comanda o desligamento da planta em caso de desenergização das saídas. Esta hipótese corresponde à adoção de uma condição "fail safe" para o sistema de intertravamento, condição esta que deverá ser programada no sistema.

O diagrama de transições para as condições de "falha crítica" (Indisponível) e de "desligamento espúrio" do sistema está apresentado na

Figura IV.11. Os estados estão representados em função do estado individual de cada canal que compõe o sistema. Os sete estados do sistema indicados na Figura são definidos como:

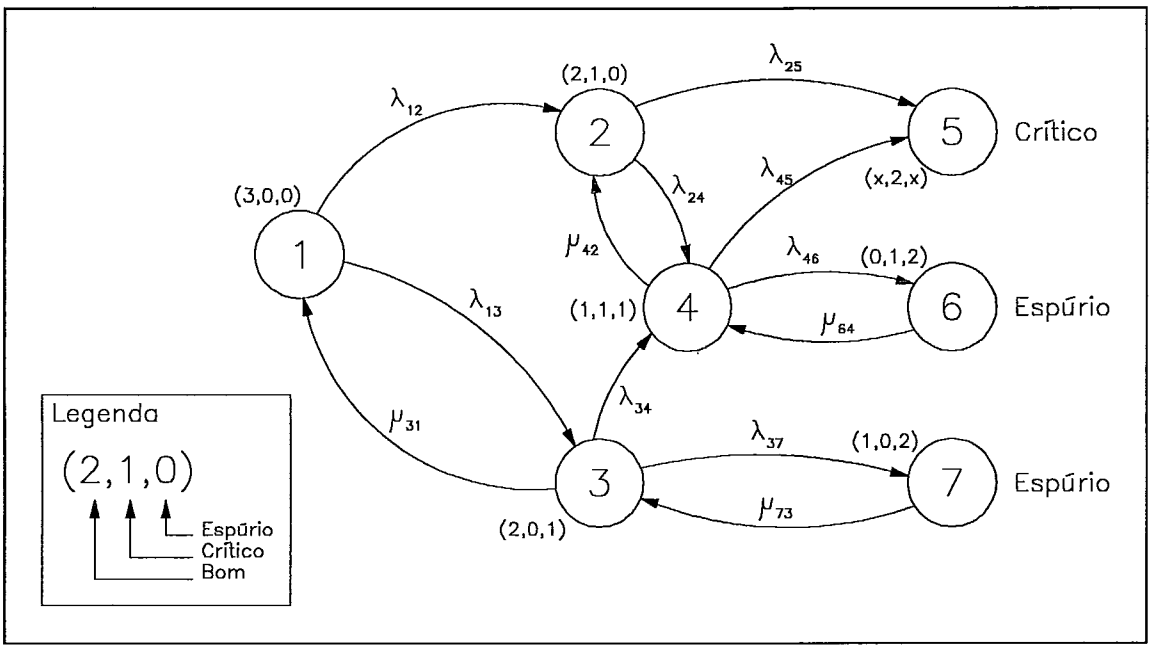


Figura IV.11 - Diagrama de Estados para Configuração TRIPLEX

- Estado 1: o sistema está perfeito (todos os componentes do sistema estão funcionando corretamente),

- Estado 2: Um CLP está em estado crítico, isto é, com falha em curto não detectado;

- Estado 3: Um CLP está em estado espúrio (entra em reparo);

- Estado 4: Um CLP está em estado espúrio (em manutenção), e outro em estado crítico;

- Estado 5: Dois ou mais CLPs estão em estado crítico, portanto o sistema está em estado crítico (não detectado);

- Estado 6: Neste estado dois CLPs estão em estado espúrio e um em estado crítico, gerando uma falha espúria do sistema;

- Estado 7: Dois CLPs em estado espúrio, gerando uma falha espúria do sistema.

Tabela IV.1 - Modos de Falha dos Componentes do CLP

Componente	Tx. de falha	Descrição	Efeito da Falha
Cartão de Entrada	$\lambda^{c}_{E,u}$ $\lambda^{a}_{E,u}$	Curto não detectado Circuito aberto não detectado	Falha Crítica Falha Espúria
Cartão de Saída	$\lambda^{c}_{S,u}$ $\lambda^{a}_{S,u}$	Curto não detectado Circuito aberto não detectado	Falha Crítica Falha Espúria
Trilho de Entrada e Saída	$\lambda^{c}_{T,u}$ $\lambda^{a}_{T,u}$ $\lambda_{T,d}$	Curto não detectado Circuito aberto não detectado Falha detectada	Falha Crítica Falha Espúria Falha Espúria
Cabeça Local	$\lambda^{c}_{L,u}$ $\lambda^{a}_{L,u}$ $\lambda_{L,d}$	Curto não detectado Circuito aberto não detectado Falha detectada	Falha Crítica Falha Espúria Falha Espúria
Cabeça Remota	$\lambda^{c}_{R,u}$ $\lambda^{a}_{R,u}$ $\lambda_{R,d}$	Curto não detectado Circuito aberto não detectado Falha detectada	Falha Crítica Falha Espúria Falha Espúria
Fonte da Cabeça Local	λ_{FL}	Falha de alimentação Cabeça	Falha Espúria
Fonte da Cabeça Remota	λ_{FR}	Falha de alimentação Cabeça	Falha Espúria
CPU	$\lambda^{c}_{C,u}$ $\lambda^{a}_{C,u}$ $\lambda_{C,d}$	Curto não detectado Circuito aberto não detectado Falha detectada	Falha Crítica Falha Espúria Falha Espúria
Interface E/S Rem. CPU	$\lambda^{c}_{I,u}$ $\lambda^{a}_{I,u}$ $\lambda_{I,d}$	Curto não detectado Circuito aberto não detectado Falha detectada	Falha Crítica Falha Espúria Falha Espúria
Fonte da CPU	λ_{FC}	Falha de alimentação CPU	Troca Espúria
Relé do votador	λ^{c}_{RV} λ^{a}_{RV}	Curto não detectado Circuito aberto não detectado	Falha Crítica Falha Espúria

De acordo com o método de Markov, o seguinte sistema de equações pode ser deduzido do diagrama mostrado na Figura IV.11:

$$\frac{dP_1(t)}{dt} = -(\lambda_{12} + \lambda_{13})\, P_1(t) + \mu_{31}\, P_3(t) \qquad \text{(IV.1)}$$

$$\frac{dP_2(t)}{dt} = \lambda_{12}\, P_1(t) - (\lambda_{24} + \lambda_{25})\, P_2(t) + \mu_{42}\, P_4(t) \qquad \text{(IV.2)}$$

$$\frac{dP_3(t)}{dt} = \lambda_{13}\, P_1(t) - (\lambda_{34} + \lambda_{37} + \mu_{31})\, P_3(t) + \mu_{73}\, P_7(t) \qquad \text{(IV.3)}$$

$$\frac{dP_4(t)}{dt} = \lambda_{24} P_2(t) + \lambda_{34}\, P_3(t) - (\lambda_{45} + \lambda_{46} + \mu_{42})\, P_4(t) + \mu_{64}\, P_6(t) \qquad \text{(IV.4)}$$

$$\frac{dP_5(t)}{dt} = \lambda_{25}\, P_2(t) + \lambda_{45}\, P_4(t) \qquad \text{(IV.5)}$$

$$\frac{dP_6(t)}{dt} = \lambda_{46}\, P_4(t) - \mu_{64}\, P_6(t) \qquad \text{(IV.6)}$$

$$\frac{dP_7(t)}{dt} = \lambda_{37}\, P_3(t) - \mu_{73}\, P_7(t) \qquad \text{(IV.7)}$$

Nas equações acima os valores de μ_{31}, μ_{42}, μ_{64} e μ_{73} são a taxa de reparo de um subsistema e $P_i(t)$, i = 1 a 7, representa a probabilidade do sistema estar no Estado i no instante t, sendo as taxas de transição definidas abaixo:

$$\lambda_d = \lambda_{T,d} + \lambda_{L,d} + \lambda_{R,d} + \lambda_{FL} + \lambda_{FR} + \lambda_{C,d} + \lambda_{I,d} + \lambda_{FC} \qquad \text{(IV.8)}$$

$$\lambda_u^a = \lambda_E^a + \lambda_S^a + \lambda_{T,u}^a + \lambda_{L,u}^a + \lambda_{R,u}^a + \lambda_{C,u}^a + \lambda_{I,u}^a + \lambda_{RV}^a \qquad \text{(IV.9)}$$

$$\lambda_u^c = \lambda_E^c + \lambda_S^c + \lambda_{T,u}^c + \lambda_{L,u}^c + \lambda_{R,u}^c + \lambda_{C,u}^c + \lambda_{I,u}^c + \lambda_{RV}^c \qquad \text{(IV.10)}$$

$$\lambda_{12} = 3\, \lambda_u^c \qquad \text{(IV.11)}$$

$$\lambda_{13} = 3\ \lambda_d + 3\ \lambda_u^a \tag{IV.12}$$

$$\lambda_{24} = 2\ \lambda_d + 2\ \lambda_u^a \tag{IV.13}$$

$$\lambda_{25} = 2\ \lambda_u^c \tag{IV.14}$$

$$\lambda_{34} = 2\ \lambda_u^c \tag{IV.15}$$

$$\lambda_{37} = 2\ \lambda_d + 2\ \lambda_u^a \tag{IV.16}$$

$$\lambda_{45} = \lambda_u^c \tag{IV.17}$$

$$\lambda_{46} = \lambda_d + \lambda_u^a \tag{IV.18}$$

Devido à dependência das Equações (IV.1) a (IV.7), para se resolver este problema é necessário lembrar que:

$$\sum_{i=1}^{7} P_i(t) = 1 \tag{IV.19}$$

Conforme mencionado anteriormente, o atributo de confiabilidade de interesse no caso da condição de falha crítica é a indisponibilidade média do sistema em um determinado período de tempo (por exemplo, um ano). Neste caso, a indisponibilidade média corresponde ao valor médio da probabilidade do sistema estar no Estado 5 (estado falho). Portanto, a indisponibilidade média em um determinado período é igual a:

$$\bar{A}(t) = \frac{1}{T} \int_0^T P_5(t)\ dt \tag{IV.20}$$

Para a condição de "desligamento espúrio", o atributo de confiabilidade de interesse é a freqüência de ocorrência de desligamentos espúrios devido a falhas espúrias dos componentes do sistema. No presente caso, esta freqüência é dada pela expressão:

$$\phi_e = \frac{1}{T} \int_0^T \{ (\lambda_d + \lambda_u^a) \cdot (P_4(t) + 2P_3(t)) \} \, dt \qquad \text{(IV.21)}$$

IV.3 - Caso Exemplo: Sistema de Detecção de Incêndio em Plataformas Marítimas

Como aplicação da Análise de Custo-Benefício, será apresentada uma aplicação de CLPs formando um sistema de monitoração de incêndio de uma zona de risco de uma plataforma de petróleo. A zona escolhida é uma das responsável pela extração de óleo, que é feita por intermédio de válvulas conhecidas como árvore de natal. Esta zona é considerada de risco em virtude da presença de gases e vapores de hidrocarbonetos.

IV.3.1 - Descrição do sistema de geração de sinais

O sistema de detecção de incêndio da Cabeça dos Poços é composto 3 subsistemas distintos, a saber:

- Sistema de detecção de chama, composto por 4 detectores de UV ligados em votação 2-de-4. Para que haja a ativação do sinal de presença de chama é necessário que pelo menos dois detectores de UV sejam sensibilizados. Um sinal de chama vindo de apenas um detector de UV gera um alarme que alerta o operador;

- Sistema eletrônico de detecção de calor, composto por 42 detectores de calor ligados em votação 1-de-42;

- Sistema de detecção de calor por plug-fusíveis, composto por uma malha de 31 plug-fusíveis ligados em votação 1-de-

31;

- Sistema de Acionamento Manual, composto por quatro chaves manuais ("Push-Buttons") instaladas na Área.

Uma descrição sucinta de cada um desses sistemas é apresentada a seguir.

IV.3.2 - Sistema de Detecção de Chama

O Sistema de Detecção de Chama é formado por 4 detectores de UV ligados a um monitor de UV. A votação 2-de-4 é feita pelo monitor de UV. Qualquer sinal de chama que sensibilize dois ou mais detectores irá gerar o sinal de incêndio confirmado.

Cada detector de UV está ligado ao monitor por intermédio de um cabo multivias de 4 condutores (5 condutores contando-se a blindagem). No caso em estudo, foi estimado que, entre o monitor e o detector existam 24 pontos de ligação (conexões). Devido ao mecanismo de ligação entre o monitor e o detector de UV, qualquer falha nesta ligação, ou seja um curto ou circuito aberto, é imediatamente detectada pelo monitor.

A saída do monitor é um contato de relé ligada à lógica de acionamento do painel de fogo e gás.

IV.3.3 - Sistema Eletrônico de Detecção de Calor

O sistema eletrônico de detecção de calor é formado por 5 malhas, onde estão distribuídos um total de 42 sensores de calor. Qualquer uma das malhas que apresentar um sinal de presença de calor irá acionar o sinal de fogo confirmado, ou seja, trata-se de uma votação 1-de-42.

Cada malha é constituída por um circuito monitor de calor, até 10 detectores e a linha que liga os detectores de uma dada malha ao monitor da mesma malha. O monitor de calor serve para verificar a integridade da linha (com respeito a uma possível descontinuidade na mesma) e acionar o alarme de

fogo.

O cabo que forma a linha tem duas vias, e o número de interconexões existentes nesta linha depende do número de detectores existentes na malha. Ao final da linha é ligada uma resistência de terminação, por onde circula uma pequena corrente de monitoração. Esta corrente possibilita ao monitor de calor detectar uma possível interrupção na linha. Um curto na linha é interpretado pelo monitor como um sinal de calor vindo de algum dos detectores, gerando assim um sinal espúrio de fogo confirmado.

A saída do monitor de calor é um sinal elétrico, ligado à lógica de acionamento do painel de fogo e gás.

IV.3.4 - Sistema de Detecção de Calor por Plug-fusíveis

O sistema de detecção de calor por plug-fusíveis é formado por um circuito pneumático monitorado por um pressostato. O circuito pneumático é formado por duas válvulas, responsáveis pela manutenção da pressurização do circuito, a linha propriamente dita e 31 plug-fusíveis. Quando na ocorrência de um incêndio, o plug-fusível mais próximo ao fogo funde, desobstruindo um orifício existente no corpo do próprio plug-fusível. Este orifício quando aberto causa a queda da pressão no circuito pneumático que é detectada pelo pressostato.

O pressostato é ligado, através de um cabo de duas vias, a um monitor semelhante ao monitor usado nos detectores de calor. Este monitor, de forma análoga aos detectores de calor, é capaz de detectar as falhas em circuito aberto que possam ocorrer no cabo de conexão com o pressostato. Um curto neste cabo será interpretado pelo monitor como um sinal de baixa pressão no circuito pneumático, gerando assim um sinal espúrio de fogo confirmado. No caso em estudo, existem 12 interconexões (ou emendas) no referido cabo.

IV.3.5 - Sistema de Acionamento Manual

O sistema de acionamento manual é formado por um circuito elétrico onde estão ligadas 4 chaves manuais do tipo "Push-Buttons". Este circuito é ligado, através de um cabo de duas vias, a um monitor semelhante ao

monitor usado nos detectores de calor. Este monitor, de forma análoga aos detectores de calor, é capaz de detectar as falhas em circuito aberto que possam ocorrer no cabo de conexão com o pressostato. Um possível curto circuito neste cabo será interpretado pelo monitor como o acionamento de uma das chaves do circuito, gerando assim um sinal espúrio de fogo confirmado. No caso em estudo, existem 12 interconexões (ou emendas) no referido cabo.

IV.3.6 - Lógica de Acionamento do Painel de Fogo e Gás

Todos os sinais gerados pelos subsistemas são enviados a um CLP responsável pela geração do sinal de incêndio confirmado. Este equipamento é denominado Gerador da Lógica de Acionamento do Painel de Fogo e Gás. Esta lógica de acionamento é implementada com o uso de instruções programadas no CLP.

O caminho do sinal é igual para todos os equipamentos envolvidos, ou seja, o sinal gerado pelos detectores é enviado ao respectivo monitor (responsável pela monitoração da linha, manipulação de sinais gerados pelo detector e votação) e, em seguida, remetido a um cartão de entrada do CLP, que é responsável pela geração do sinal de fogo confirmado.

IV.4 - Árvore de Falhas do Sistema de Detecção de Incêndio

Para a análise da confiabilidade da Cabeça dos Poços devem ser calculados dois atributos, a saber:

- **Indisponibilidade Média** que é a probabilidade de que o sistema de detecção de incêndio não esteja disponível quando da ocorrência de um incêndio na Cabeça dos Poços, em virtude de alguma falha do sistema ou devido a manutenção corretiva de um dos seus subsistemas;

- **Freqüência de Acionamentos Espúrios** que é a freqüência de ocorrência de acionamentos do sinal de fogo confirmado devido a apenas falhas intrínsecas do sistema, sem que haja uma real situação de incêndio.

IV.4.1 - Avaliação da Indisponibilidade Média

A **indisponibilidade média** do sistema de detecção de incêndio da Cabeça dos Poços é devido a duas componentes:

- a indisponibilidade devido a falhas em operar do sistema, ou seja falhas não detectáveis (ou detectadas apenas na demanda ou em testes periódico);

- a indisponibilidade devido a manutenção de um dos sub-sistemas de monitoração (manutenção devido a falhas detectáveis do sistema).

A primeira componente da indisponibilidade média, ou seja, indisponibilidade média devido a falhas em operar do sistema, ou a probabilidade do sistema não responder a uma demanda real de incêndio, pode ser calculada pela expressão (Oliveira, 1985) (para os componentes testados periodicamente):

$$\overline{A} = 1 - \frac{1}{\lambda\theta}(1-e^{-\lambda\theta}) + \lambda\tau \qquad \text{(IV.22)}$$

onde, λ é a taxa de falha do componente (para o modo de falha "falha em operar quando demandado"), θ o intervalo entre testes e τ o tempo de reparo.

A partir do estudo do alcance dos detectores e dos plug-fusíveis, a área da cabeça dos poços foi dividida em sub-áreas, sendo cada uma delas protegidas por:

- um detector de calor;
- um plug-fusível;
- dois detectores de UV ligados em lógica 2-de-2;
- uma chave manual.

Os argumentos usados para estabelecer o modelo acima foram os seguintes:

- No "Manual de Instruções de Operação, Manutenção e Teste do Sistema de Detecção de fogo e gás da Plataforma

de Produção de Petróleo " a faixa de atuação do detector de UV está compreendida em um cone de visão de 80º, com maior sensibilidade em seu eixo central, com um comprimento de 15 metros. Assim sendo é razoável admitir-se que pelo menos dois dos quatro detectores de UV localizados nesta área conseguem "visualizar" qualquer região da cabeça dos poços;

- De acordo com o mesmo manual referido acima, os detectores de calor foram instalados na plataforma de forma que a área coberta por cada um deles não ultrapasse 25 m^2. Na área da cabeça dos poços, cada detector de calor está cobrindo, em média, uma área próxima a este valor.

- A malha de plug-fusíveis localizada nesta área é formada por 31 plugs distribuídos uniformemente. Admitiu-se que qualquer região da área da cabeça dos poços é monitorada por um plug-fusível.

A segunda componente da indisponibilidade média, ou seja, indisponibilidade média devido às manutenções corretivas dos componentes, ou a probabilidade do componente estar sendo submetido a uma manutenção corretiva, pode ser calculada pela expressão (Oliveira, 1985):

$$\overline{A} = \frac{\lambda\tau}{\lambda\tau + 1} - \frac{\lambda\tau^2}{(\lambda\tau+1)^2 T}\left(1 - e^{-(\lambda+\frac{1}{\tau})T}\right) \qquad \text{(IV.23)}$$

onde, λ é a taxa de falha do componente (das falhas detectadas), τ o tempo de reparo e T é o intervalo de tempo para o qual a indisponibilidade média está sendo calculada (T = 8760 h, neste trabalho).

Para efeito da construção da árvore de falhas da indisponibilidade média considerou-se que:

- O sistema de detectores de UV estará em manutenção

corretiva quando pelo menos uma das oito entradas do monitor de UV indicar uma falha detectada;

- O sistema de detectores de calor estará em manutenção corretiva quando a linha de entrada do monitor de calor apresentar um circuito aberto;
- O sistema de detecção por plug-fusíveis, estará em manutenção corretiva quando a linha de entrada do monitor do pressostato apresentar um circuito aberto.

A justificativa para essas considerações são as seguintes:

- O monitor de UV possui oito entradas e cada uma delas é uma possível fonte de falhas detectadas, ou seja, uma falha em qualquer um dos detectores ligados ao monitor fará com que o monitor seja desabilitado para que o detector falho seja consertado;

- Os detectores de calor são ligados a uma linha comum que é o caminho de comunicação entre eles e o monitor de calor. As possíveis falhas detectadas do sistema são decorrentes de defeitos na linha de comunicação, mais precisamente as falhas detectadas são as falhas em circuito aberto. A maior fonte de falhas em circuito aberto em cabos ocorrem nas juntas ou interconexões do mesmo. Isto torna cada um dos detectores de calor uma possível fonte de falhas detectadas, pois a instalação de um detector em um determinado ponto da linha acarreta uma emenda neste ponto. Nesta zona a detecção de calor é feita por 5 malhas com uma média de 8 detectores cada. Quando ocorre uma falha detectada a linha correspondente fica indisponível até que ela seja reparada;

- No caso da malha de plug-fusíveis, o único elemento monitorado (ou seja com capacidade de detecção de falhas) é a linha que liga o pressostato ao monitor do pressostato (monitor de linha). O mecanismo é semelhante ao mecanismo descrito acima, ou seja, as falhas em circuito aberto são detectáveis. Os elementos que podem mais

causar falhas deste tipo são as juntas ou emendas dos cabos.

IV.4.2 - Avaliação da Freqüência de Acionamentos Espúrios

O valor da freqüência de acionamentos espúrios de cada componente é medido pelo número de falhas esperados para um determinado período, que pode ser calculada pela seguinte equação (Oliveira, Frutuoso e Gamal, 1991):

$$W(0,t) = \frac{\lambda\mu}{\lambda+\mu}t + \frac{\lambda^2}{(\lambda+\mu)^2}[1-e^{-(\lambda+\mu)t}] \qquad \text{(IV.24)}$$

onde W(0,t) é o número de falhas esperado para o período de 0 a t, λ é a taxa de falha do componente para o modo de falha "operação espúria ou indevida" e μ é a taxa de reparo. Como pode ser observado na prática, geralmente $\mu >> \lambda$, resultando na seguinte aproximação :

$$W(0,t) \approx \lambda t \qquad \text{(IV.25)}$$

Em alguns casos, é necessário também, o cálculo da probabilidade de que um segundo evento espúrio ocorra durante um intervalo determinado. O cálculo desta probabilidade de ocorrência é efetuado com o uso da seguinte expressão (Oliveira, 1985):

$$P_e(\Delta T) = 1 - e^{-\lambda_e \Delta T} \approx \lambda_e \Delta T \qquad \text{(IV.26)}$$

onde λ_e é a taxa de falha espúria do componente, ΔT é a tempo de exposição à falha, que é o intervalo de tempo em que o sistema está sujeito a uma falha deste tipo.

Para fins da avaliação da freqüência de acionamentos espúrios, da Cabeça dos Poços foi modelada como uma única zona, onde estão localizados todos os equipamentos responsáveis pela geração de um sinal espúrio. Assim sendo a modelagem da Cabeça dos Poços é a seguinte:

- Quatro detectores de UV ligados em lógica 2-de-4 a um monitor de UV;

- 31 plug-fusíveis ligados a um circuito pneumático e monitorados por um pressostato (pressostato ligado a um monitor de linha);
- 42 detectores de calor ligados em 5 malhas com um monitor de calor em cada malha;
- 4 chaves manuais ligadas a um monitor de linha.

Todos os componentes dos subsistemas de detecção de calor e plug-fusíveis (chaves, detectores, plugs, circuito pneumático, pressostatos, cabos e monitores), são capazes de sozinhos causar um acionamento espúrio. Para o subsistemas de detectores de UV (chama) o mecanismo de geração de falha espúria é um pouco mais complexo. A falha pode ocorrer nas seguintes situações:

- O monitor de UV falha gerando um sinal espúrio;
- Um dos detectores de UV falha gerando um alarme (devido a votação 2-de-4 é necessário que mais de um detector falhe para que haja a geração do sinal de fogo confirmado). No intervalo de tempo que o operador ainda não desabilitou o monitor de UV (de forma a prevenir a ocorrência de uma geração do sinal de fogo confirmado espúrio devido a uma falha em um outro detector) um dos outros 3 detectores falha causando um sinal espúrio. Neste trabalho, estima-se que o tempo médio para que o operador desabilite o monitor de UV é de 15 minutos.

As árvores de falhas para a indisponibilidade média e freqüência de acionamentos espúrios, respectivamente, para as configurações sugeridas são mostradas nos apêndices A e B. O Cálculo de indisponibilidade média e freqüência de acionamentos espúrios, para cada configuração de CLP, são feitos pelo método markoviano e o resultado é colocado como uma probabilidade, ou freqüência, conforme o caso, diretamente na árvore de falhas.

IV.4.3 - Dados de falhas

A construção e a avaliação quantitativa das árvores de falhas desenvolvidas neste trabalho foram realizadas utilizando-se um programa de cálculo de árvore de falhas. Estes dados, utilizados para alimentar o programa,

são apresentados na Tabela IV.2. Na Tabela IV.2 são descritos os modos de falha de cada um dos componentes.

Tabela IV.2 - Dados de Falha

Componente	Modo de Falha	Dados de Falha	Fonte
Chaves	FOD	λ = 0.0126E-6	(IEEE, 1977)
	SE	λ = 0.085E-6	(IEEE, 1977)
Pressostatos	FOD	λ = 3.2E-6 /h	(OREDA, 1984)
	SE	λ = 1.9E-6 /h	(OREDA, 1984)
Detector de Calor	FOD	λ = 2.7E-7 /h	(SINTEF, 1986)
	SE	λ = 1.0E-6 /h	(SINTEF, 1986)
Detector de UV	FOD	λ = 3.5E-6 /h	(OREDA, 1984)
	SE	λ = 5.7E-6	(OREDA, 1984)
	MAN	λ = 0.4E-6 /h	(OREDA, 1984)
Monitor de UV	FOD	λ = 2.3E-6 /h (por canal)	(OREDA, 1984)
	SE	λ = 7.3E-6 /h	(OREDA, 1984)
	MAN	λ = 18E-6 /h	(OREDA, 1984)
Monitores de Calor e Pressostatos	FOD	λ = 1.24E-6 /h	(MIL,1982), (NPRD2, 1981)
	SE	λ = 1.39E-6	(MIL,1982), (NPRD2, 1981)
Plug-Fusível	FOD	λ = 1.3E-7	(OREDA, 1984)
	SE	λ = 1.3E-7	(OREDA, 1984)
Juntas do Cabeamento	ALL	λ = 3.51E-7 (por junta)	(NPRD2, 1981)
Válvula Tri-Way	RPT	λ = 11.42E-6	(Rijmnond)
Juntas de canos	RPT	λ = 5.7E-8	(Lees, 1980)
Operador	FOD	PROBABILIDADE = 0.1	Especialistas
Desabilitação da Malha de UV para execução de Soldas	DESABIL	PROBABILIDADE = 0.112	Especialistas

Tabela IV.3 - Modos de Falhas dos Componentes

Código	Modo de Falha
FOD	Falha em operar na demanda (nos instantes iniciais do acidente)
SE	Falha que gera sinal espúrio
RPT	Ruptura
MAM	Falha que acarreta em manutenção corretiva

IV.5 - Análise Custo-Benefício

A Análise Custo-Benefício será realizada considerando-se cada uma das configurações definidas no capítulo III. Esta análise custo-benefício consiste no levantamento dos custos e benefícios resultantes da utilização de cada uma das configurações analisadas. O balanço econômico dos custos e benefícios indicará se a configuração é recomendável ou não: se positivo, indica que haverá um ganho líquido anual (lucro) e, portanto, a configuração é recomendável.

Os custos associados às configurações são relacionados à instalação dos equipamentos, aos custo de capital e manutenção dos mesmos. O cálculo do benefício de cada configuração é efetuado computando-se a redução das perdas esperadas devido a acidentes, levando-se em consideração as perdas decorrentes das falhas espúrias provocadas pelo sistema.

A seguir são apresentados em detalhe a avaliação dos custos e benefícios para cada uma das configurações.

IV.5.1 - Avaliação dos Benefícios

Como foi mostrado na seção II.5.2, para avaliação dos benefícios decorrentes da instalação de uma dada configuração, são necessários alguns parâmetros que traduzem, basicamente, o nível das perdas decorrentes dos aci-

dentes monitorados e pela introdução do sistema de monitoramento. Para o caso exemplo, Sistema de Detecção de Incêndio da Cabeça dos Poços, estes dados são os seguintes:

a) Freqüência de ocorrência de incêndios na zona em evidência:

   Este dado é calculado a partir de dados históricos (WOAD, 1990) e a sua avaliação está apresentada no Apêndice E. O valor utilizado neste trabalho é 1.80×10^{-2} incêndios/ano;

b) Perda econômica média por incêndio:

   O valor utilizado neste trabalho corresponde ao prêmio médio pago pela companhia de seguro. Este valor foi fornecido por especialistas é equivalente a US$ 300.000.000,00 (trezentos milhões de dólares);

c) Perda humana média por incêndio:

   Este dado foi obtido a partir de dados históricos (WOAD, 1990) e o valor utilizado neste trabalho corresponde a 0,172 vidas/incêndio;

d) Perda econômica devido a falha espúria:

   O valor utilizado foi obtido a partir de consultas a especialistas e seu cálculo está apresentado no Apêndice F. O valor utilizado neste trabalho é equivalente a US$ 56.688,85 dólares/falha espúria.

e) Valor da vida humana:

   Para fins deste trabalho foi utilizado o valor de US$ 10.000.000,00. Este valor é tradicionalmente utilizado em análises feitas para a indústria nuclear.

A partir dos dados acima, pode-se calcular qual seria a perda média anual, em dólares ou em termos de vidas humanas, para zonas de cabeças de poços de plataformas sem nenhum tipo de sistema de proteção.

Para tanto utilisa-se a equação (II.20), fazendo-se indisponibilidade do sistema de proteção ($\bar{A}$) igual a zero. Assim, as perdas obtidas são:

Perda econômica média anual :	US$ 5.430.960,00
Perda humana média anual:	3.1×10^{-3} vidas

Com a instalação do equipamento de monitoração (malha de sensores e CLPs), as perdas mostradas acima sofrerão uma redução correspondente aos incêndios detectados. Permanecerá, devido a indisponibilidade do sistema, uma pequena parcela de acidentes que não serão detectados.

Embora o sistema de proteção traga como um benefício direto a redução dos prejuízos causados por incêndios. Em contrapartida, as falhas espúrias deste mesmo sistema, causará uma redução do benefício que deve ser computado.

A avaliação dos benefícios e perdas residuais, alcançados por cada configuração de CLP, calculados através das equações (II.18) e (II.20), são mostrados na tabela IV.4, mostrada abaixo:

Tabela IV.4 - Benefícios e Perdas Residuais de Cada Configuração

Configuração	SIMPLEX	DUAL SIMPLEX	DUAL DUAL 1-2	DUAL DUAL 2-2	TRIPLEX 2-3
Indisponibilidade	2.74×10^{-2}	2.87×10^{-2}	3.60×10^{-3}	5.40×10^{-2}	5.31×10^{-3}
Freqüência de Acionamentos Espúrios (acionamentos/ano)	1.74	1.27	2.75	0.84	0.84
Benefício anual direto (US$/ano)	5.282.043,08	5.274.982,83	5.411.386,.82	5.137.579,54	5.402.099,88
Redução do benefício devido a falhas espúrias (US$/ano)	98.638,60	71.994,84	155.894,34	47.618,63	47.618,63
Benefício líquido (US$/ano)	5.183.404,48	5.202.987,99	5.255.492.48	5.089.960.91	5.354.481.24
Perda Econômica Residual (US$/ano)	179.028,00	186.048,00	50.421,60	322.668,00	59.655,60
Benefício para segurança (mortes evitadas/ano)	3.01×10^{-3}	3.01×10^{-3}	3.08×10^{-3}	2.93×10^{-3}	3.08×10^{-3}
Risco residual (mortes/ano)	8.49×10^{-5}	8.89×10^{-5}	1.12×10^{-5}	1.67×10^{-4}	1.65×10^{-5}

Os atributos de confiabilidade para o sistema de proteção,

utilizados na Tabela IV.4, foram obtidos através das árvores de falhas apresentadas no Apêndices A e B, conforme a metodologia mostrada no capítulo III.

Os dados mostrados na Tabela IV.4 representam as principias características de cada configuração. O benefício anual direto representa a o prejuízo evitado pelo sistema de proteção, que é uma composição dos prejuízos econômicos (equipamentos e instalações) somados aos sociais (vidas expressas em valores monetários). A redução de benefício devido a falhas espúrias representa os prejuízos decorrentes das paradas espúrias causadas pelo sistema de proteção. Esta parcela é deduzida da primeira resultando no benefício líquido. A perda econômica residual é aquela decorrente da indisponibilidade do sistema de proteção. O número de mortes evitadas pelo sistema de proteção é representado pelo benefício para segurança. O Risco residual é o número de mortes esperadas devido a indisponibilidade do sistema de proteção.

IV.5.1 - Avaliação dos Custos

Para o cálculo dos custos de cada configuração, pode-se dividir o sistema de proteção em duas partes distintas, a saber:

- subsistema de geração de sinais; e
- controladores lógicos programáveis.

Os custos de cada uma destas partes independem uma da outra.

Os custos de capital, instalação e manutenção do subsistema de geração de sinais (mostrado na seção IV.3.1) são avaliados no apêndice D e resumidos na Tabela IV.5, mostrada abaixo:

Tabela IV.5 - Custos do Subsistema de Sensoramento

Subsistema	Custo de Capital (US$)	Custo de Instalação (US$)	Custo de manutenção (US$/ano)	Custo Total Anualizado (US$/ano)
Fogo (Calor)	8.476,82	8.294,00	6.282,78	7.864,93
Chama (UV)	25.530,62	15.193,00	4.709,28	8.857,07
Plug-fusíveis	15.075,41	16.934,00	37,20	3.297,43
Manual	2.883,29	789,90	40,00	363,20
Total	51.966,14	41.210,90	11.069,26	20.382,63

Para obter-se os valores expressos na Tabela IV.5, na coluna de Custo Total Anualizado, as quantias expressas em termos de valor presente (ou seja, o custo de capital e o custo de instalação), foram anualizados pela fórmula (II.7) e depois somados aos custos de manutenção. Para efeitos de cálculo, utilizando a fórmula (II.7), foi admitida uma taxa de juros anuais de 8% e que a vida útil do equipamento é de 20 anos.

Para a avaliação dos custos de capital e de manutenção de cada uma das configurações de CLP, utilizou-se um critério de proporcionalidade em função da complexidade de cada configuração. Uma vez que o custo dos votadores é pequeno, quando em comparação aos demais equipamentos, pode-se facilmente constatar que as configurações DUAL-DUAL e TRIPLEX, terão custos aproximados iguais a duas e a três vezes ao da configuração SIMPLEX, respectivamente. Pelo mesmo critério, avalia-se que, o custo da configuração DUAL-SIMPLEX é aproximadamente 50% a mais que a configuração SIMPLEX. Como o custo de capital médio da configuração SIMPLEX é da ordem de US$ 30.000,00, e seus custos de manutenção são da ordem de US$ 1.000,00 por ano, pode-se obter a planilha de custos, mostrada na Tabela IV.6, onde estão representados os custos totais do CLP e do Sistema de Proteção como um todo.

Tabela IV.6 - Custos de Cada Configuração de CLP

Configuração	SIMPLEX	DUAL-SIMPLEX	DUAL-DUAL 1-2	DUAL-DUAL 2-2	TRIPLEX 2-3
Manutenção (US$/ano)	1.000,00	1.500,00	2.000,00	2.000,00	3.000,00
Custo de Capital Atual (US$)	30.000,00	45.000,00	60.000,00	60.000,00	90.000,00
Custo de Capital Anualizado (US$/ano)	3.055,57	4.583,35	8.111,13	8.111,13	9.166,70
Custo Total CLP (anualizado) (US$/ano)	4.055,57	6.083,35	10.111,13	10.111,13	12.166,70
Custo Total do Sistema (US$/ano)	24.438,19	26.465,97	28.493,75	28.493,75	32.549,32
Custo Total Presente do Sistema (US$)	239.937,73	259.846,80	279.755,88	279.755,88	319.574,02

IV.5.3 - Resultados da análise

Duas relações importantes podem ser obtidas dos resultados mostrados nas duas seções anteriores:

- Relação benefício líquido sobre custo; e
- Custo sobre morte estatisticamente evitada pelo sistema.

A primeira, diz respeito à relação entre a redução das perdas esperadas (econômicas mais as vidas humanas) e o custo da configuração. Esta relação pode mostrar qual é a opção economicamente mais indicada para uma determinada aplicação. A segunda, obtida dividindo-se o custo total anualizado da configuração pelo benefício para a segurança (redução do número de mortes estatisticamente evitada), mostra quantos dólares são investidos na tentativa de se evitar a ocorrência de uma morte estatisticamente esperada devido a incêndios na plataforma. Estes resultados são mostrados na Tabela IV.7.

De forma a facilitar a visualização dos resultados acima, as figuras IV.12 e IV.13 mostram os valores obtidos para as relações de Benefício-Custo e Dólares-Morte Estatisticamente Evitada, respectivamente. A Figura IV.14 mostra o gráfico de risco residual para cada configuração.

Como pode ser observado, na Tabela IV.6, a configuração DUAL-DUAL 2-de-2 tem custos exatamente iguais, obviamente, ao da configuração DUAL-DUAL 1-de-2, e não oferece nenhum tipo de vantagem econômica em relação a esta. A votação 2-de-2, usada neste caso, proporciona realmente uma queda substancial na freqüência de acionamentos espúrios. No entanto, esta não

é suficiente para compensar o aumento das perdas residuais. Desta forma, pode-se eliminar esta configuração e continuar a análise apenas com as demais.

Tabela IV.7 - Resultados Obtidos

Configuração	SIMPLEX	DUAL-SIMPLEX	DUAL-DUAL 1-2	DUAL-DUAL 2-2	TRIPLEX
Benefício Econômico (US$/ano)	5.282.043,08	5.274.982,83	5.411.386,.82	5.137.579,54	5.402.099,88
Benefício Segurança (Vidas/ano)	3.01E-3	3.01E-3	3.08E-3	2.93E-3	3.08E-3
Custo (US$/ano)	24.438,19	25.465,97	28.493,75	28.493,75	32.549,32
Custo em cap, Presente (US$)	239.937,73	259.846,80	279.755,88	279.755,88	319.574,02
Benefício Econômico/Custo	212,10	196,59	184,44	178,63	164,50
Dólares/Mortes Estatisticamente Evitadas (milhões de US$)	8,12	8,80	9,24	9,73	10,57

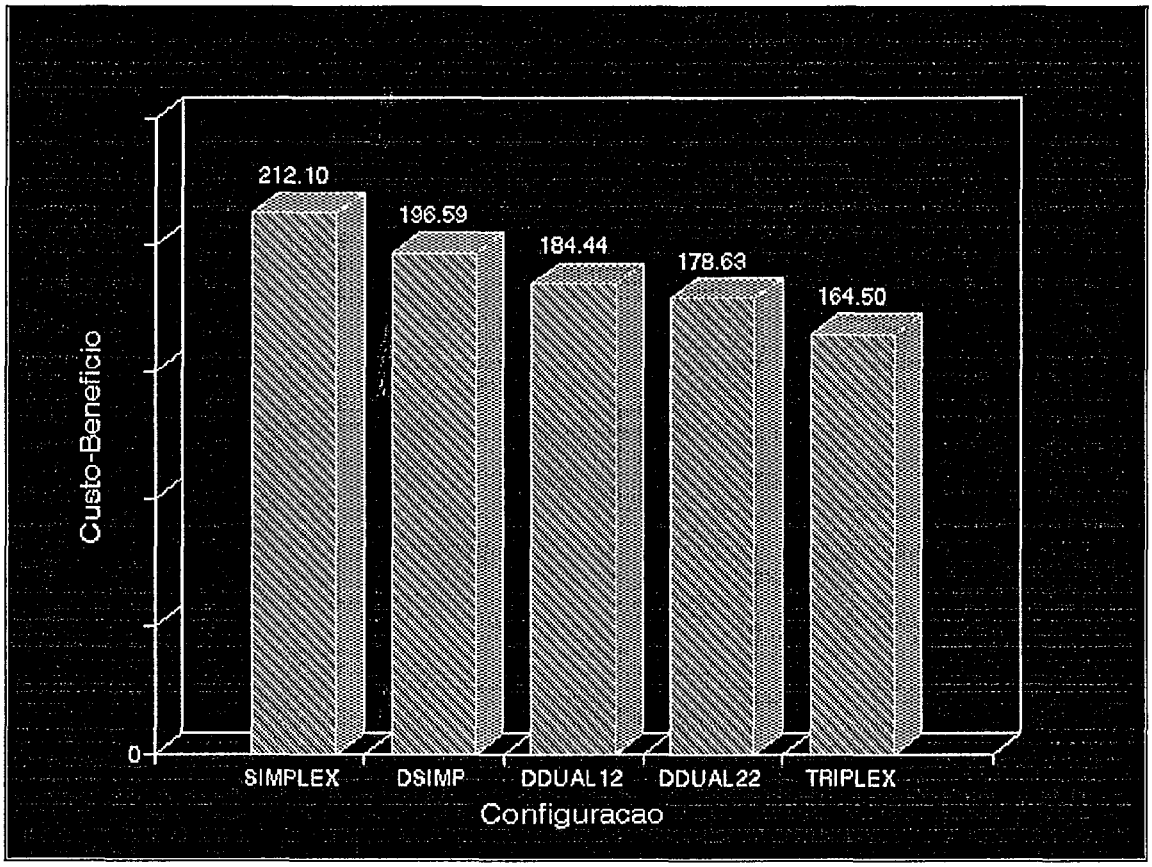


Figura IV.12 - Benefício/Custo para cada Configuração

A Figura IV.15 mostra o comportamento das variáveis perda-residual e perda por falhas espúrias em relação ao custo de cada configuração, partindo da hipótese de um sistema sem equipamento de proteção (Perda

econômica máxima, nenhuma perda por falhas espúrias e custos nulos). Na mesma figura, as variáveis são somadas compondo, assim, o nível de perda total proporcionado por cada configuração em relação ao seu custo.

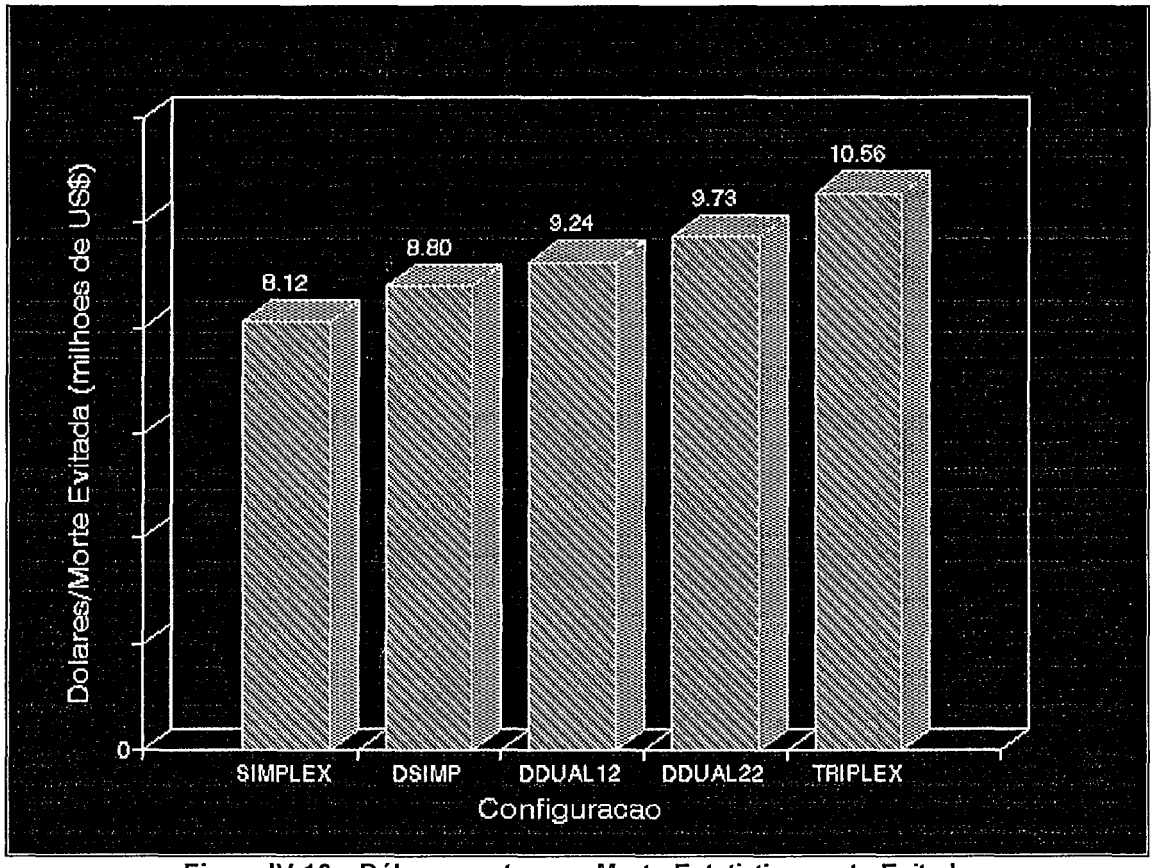


Figura IV.13 - Dólares gastos por Morte Estatisticamente Evitada

Embora todas as configurações sejam custo eficientes, ou seja proporcionem ganhos com sua instalação, a escolha da melhor configuração, não pode simplesmente se basear na escolha da solução de melhor relação benefício-custo, pois devido ao elevado valor econômico da plataforma, as soluções mais custo eficientes podem apresentar um valor de perda residual ainda muito elevado, possivelmente considerado inaceitável.

Os resultados aqui apresentados, podem auxiliar na escolha da configuração a ser utilizada se houver um valor ou critério adicional estipulado pelos projetistas, orgãos regulamentadores, ou ainda pela direção da empresa que encomenda os sistemas de proteção. Por exemplo, a curva mostrada na Figura IV.15 poderia ser utilizada para a escolha da configuração, que apresentasse perdas totais inferiores a um determinado nível considerado aceitável.

Outro exemplo que pode ser citado, é a regra ALARA ("As Low As

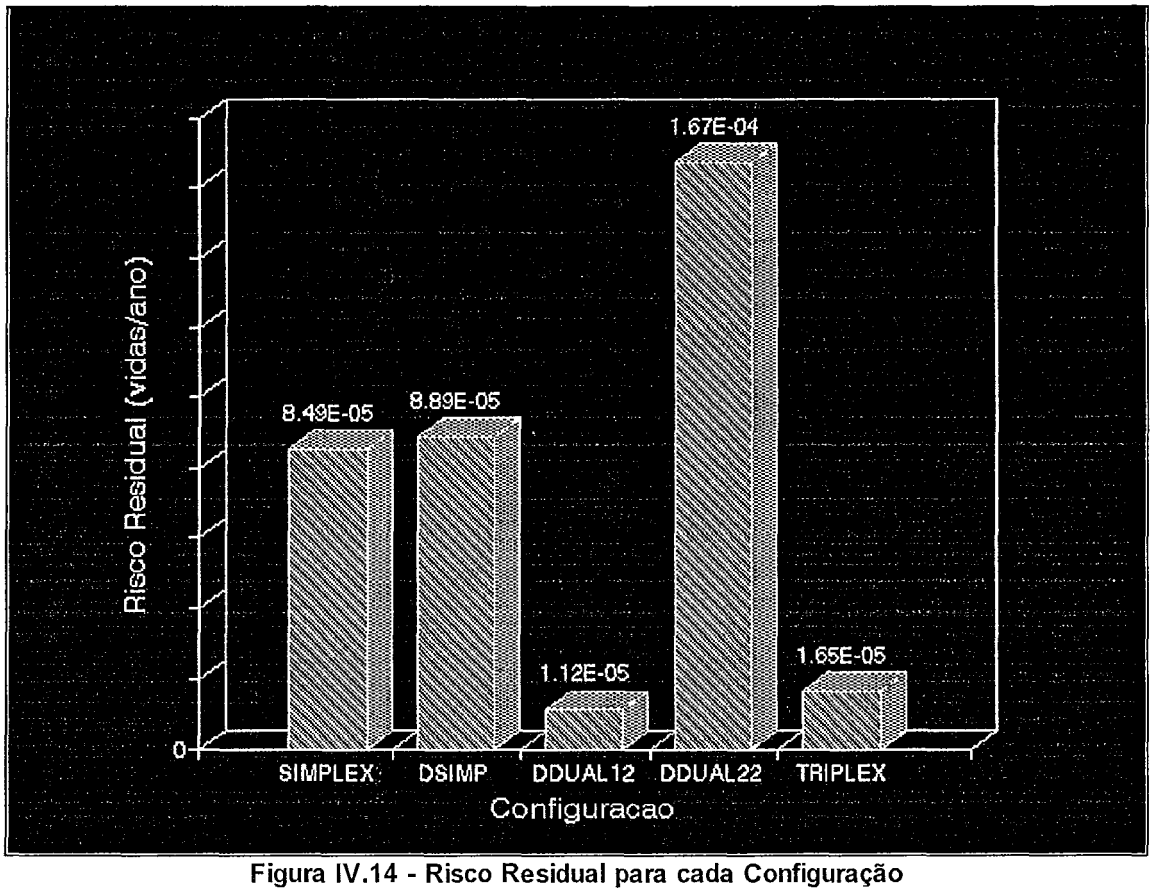


Figura IV.14 - Risco Residual para cada Configuração

Reasonnably Achievable") formulada pelo NRC ("Nuclear Regulatory Commission"), que estipula que: "Qualquer solução que apresente um custo inferior ao valor estipulado para a redução de uma morte estatisticamente esperada deve ser implementada", tipicamente a NRC estipula este valor em US$ 10 x 10^6 por morte estatisticamente evitada. Segundo esta regra, a configuração TRIPLEX, que apresenta um valor de 10,6 milhões de dólares gastos por morte estatisticamente evitada, não seria obrigatoriamente escolhida. Assim, optar-se-ia pela configuração DUAL-DUAL 1-de-2.

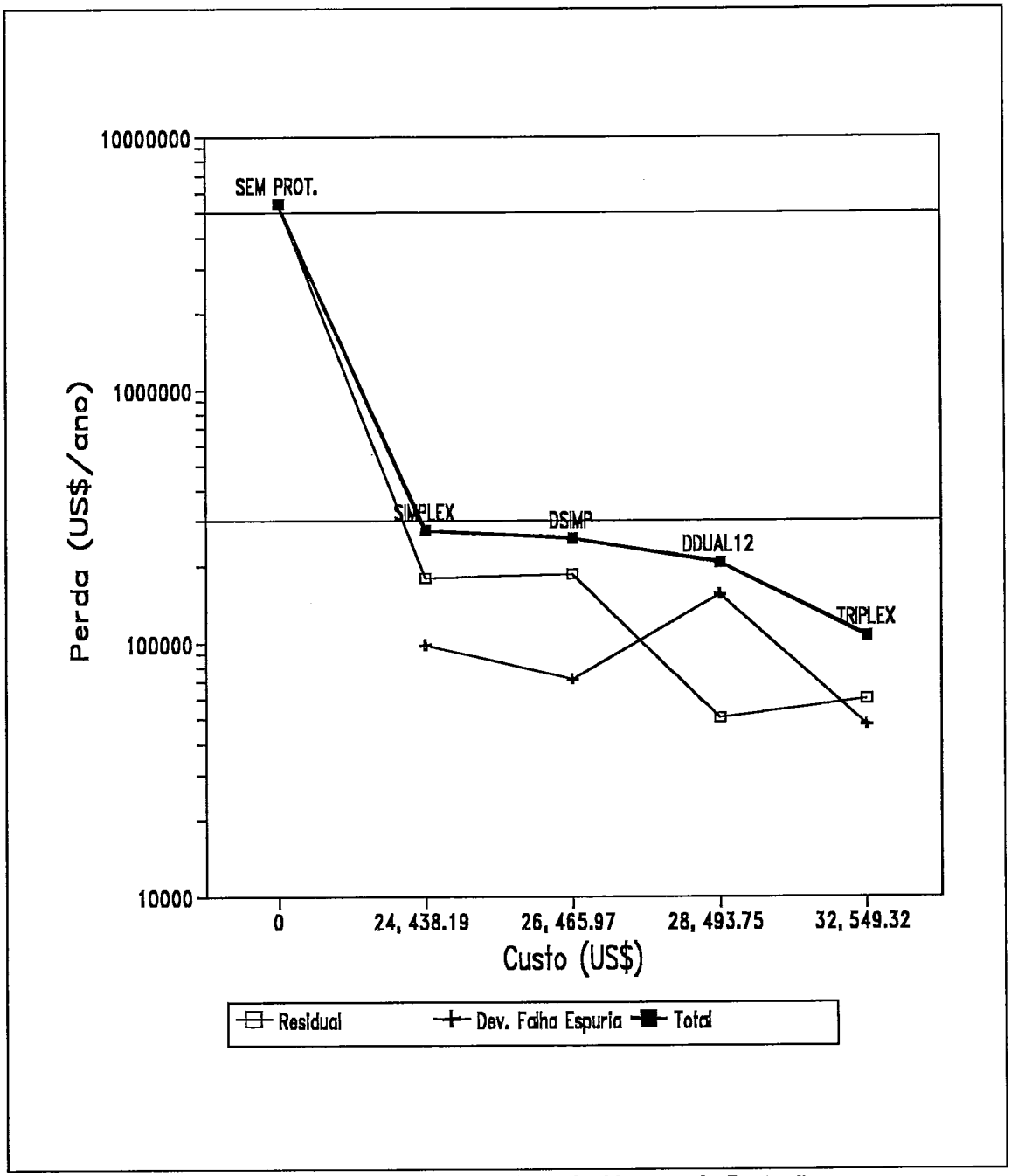


Figura IV.15 - Perdas Econômicas do Sistema de Proteção

V. CONCLUSÕES E RECOMENDAÇÕES

O objetivo deste trabalho foi a proposição de uma metodologia para Análise de Custo-Benefício de configurações de Controladores Lógicos Programáveis tolerantes a falhas, empregados em sistemas de proteção. Como caso exemplo de aplicação, foi utilizado o sistema de detecção de incêndio de uma plataforma de petróleo. Este trabalho é uma extensão às análises de confiabilidade comumente aplicadas àqueles tipos de sistemas, que em geral se restringem a levantar apenas os atributos de confiabilidade. Muitas vezes tais atributos não são suficientes para que a escolha de uma dentre várias configurações usadas para realização de uma mesma tarefa seja efetuada. Por intermédio da metodologia aqui apresentada, configurações podem ser comparadas, através dos benefícios econômicos ou sociais (segurança para instalações e pessoal) por elas oferecidos.

Nas análises de confiabilidade, realizadas para cada configuração do caso exemplo, calcularam-se os atributos **indisponibilidade** e **freqüência de acionamentos espúrios** que, agregados ao valor atribuído à vida humana, freqüência de ocorrência de incêndios e perda econômicas e sociais causadas por incêndios, quantificaram os benefícios proporcionados por cada uma das configurações. Com base no "hardware" empregado em cada configuração, os custos das mesmas puderam ser levantados.

Os resultados alcançados mostraram que todas as configurações envolvidas no caso exemplo são custo-eficientes (todas elas apresentam uma relação benefício sobre custo maior que um), sendo que uma delas, por apresentar resultados inferiores ao de outra solução de mesmo custo, pôde ser descartada.

Concluiu-se ainda que não basta comparar-se as relações benefício sobre custo, para que seja feita a escolha da melhor configuração. A escolha pode ser feita com base nos resultados obtidos, desde que um critério adicional seja estipulado, o qual pode refletir o nível de perda mínima que se deseja alcançar com o sistema de proteção. Cite-se como exemplo a apresentação da regra "ALARA" da NRC que, juntamente com os resultados obtidos, permitiu a escolha de uma dada configuração.

A questão do valor atribuído para a vida humana, embora polêmica, não foi representativa no caso exemplo. Mesmo utilizando-se um valor elevado para este parâmetro (US$ 10.000.000,00 por pessoa), o volume de recursos envolvido não implicou alterações substanciais no resultado global, dado o número reduzido de pessoas sujeitas ao evento analisado. Certamente não se pode generalizar esta conclusão, pois, em se tratando de outros casos, onde o efeito da falha do sistema envolveria um maior contingente de pessoas - como, por exemplo, indústrias químicas próximas a aglomerados populacionais - este parâmetro teria maior grau de significância.

A metodologia apresentada possui como principal características a simplicidade e versatilidade, o que possibilita a sua aplicação, tanto na área de segurança quanto na de controle de processos.

No campo da segurança, especificamente no caso exemplo, sabe-se que, cada vez mais o projetista se defronta com uma grande variedade de tipos de sensores, com princípios de funcionamento baseados em diferentes tecnologias e passíveis de serem instalados segundo as mais diversas combinações. Em tais situações, facilmente poder-se-á aplicar esta metodologia na implementação de uma análise de custo-benefício envolvendo as configurações de sistemas de sensoramento, comparando-se os vários projetos apresentados.

No campo do controle de processos, também podem ser amplas as alternativas de projetos disponíveis, os quais deverão ser analisados sob a ótica de compatibilização das variáveis "continuidade operacional" e "manutenção da especificação do produto". Como se vê, a decisão quanto ao projeto a ser implementado recairá em análise de custo-benefício que terá a confiabilidade do aparelho produtivo como "pano de fundo", e poderá fazer uso da metodologia ora apresentada como instrumental.

As dificuldades encontradas para a obtenção dos dados utilizados neste trabalho sugerem que as empresas ou orgãos interessados em análises semelhantes mantenham as informações (dados econômicos ou de confiabilidade) armazenadas na forma de bancos de dados, procedimento que facilitará uma rápida avaliação das várias alternativas para um projeto envolvendo equipamentos de segurança.

Como extensão do trabalho aqui apresentado e objetivando incre-

mentar a qualidade da análise e dos resultados obtidos, seria recomendável sofisticar a metodologia de decisão, elaborando-se uma análise de incertezas. Neste tipo de análise, as principais grandezas ou valores utilizados seriam considerados como variáveis aleatórias, às quais estariam associadas uma distribuição de probabilidades, ao invés de único valor determinístico.

BIBLIOGRAFIA

Albuquerque, R., Gamal, H., Pinto, J.E., "Análise Computadorizada de Árvores de Falhas", anais do 9º Seminário de Segurança Industrial - IBP, Rio de Janeiro, 1992.

Carrada, E., Somma, R., "Markov process in reliability", Revista Tecnica Selenia, Roma, Industrie Eletroniche Associate S.P.A.. 4(3):1-84, 1977.

Carter, W.C., Bouricius, W.G., "A survey of fault tolerant computer archicteture and its evaluation", Computer, Vol. 4, No. 1, January 1971, pp. 9-16.

Cerqueira, A.C.F.P., "Análise markoviana de confiabilidade de configurações alternativas de sistemas de bombeio", Tese de Mestrado, COPPE, UFRJ, Janeiro, 1992.

Finkel, V.S., Kirchoff, H. P., "O uso de controladores programáveis e microcomputadores em sistemas de segurança", 6º Seminário de Instrumentação do Instituto Brasileiro de Petróleo, Rio de Janeiro, outubro de 1985.

Fisher, Thomas G., "Are programmable controllers suitable for emergency shutdowsn systems?", ISA Transactions, Vol. 29, No 2, 1990.

Francisco, A. S., "Análise de confiabilidade de configurações alternativas de controladores lógicos programáveis para sistemas de segurança", Tese de Mestrado, COPPE, UFRJ, 1993.

HMSO, "PES-Programable Electronic Systems in Safety-related Applications, Parts 1-3", Heath and Safety Executive, London, UK, 1985.

IEEE, "IEEE Guide to the Collection and Presentation of Electrical, Electronic, Sensing Component, and Mechanical Equipment Reliability Data for Nuclear-Power generating Stations", New York USA, 1977.

ISA, Instrumentation Society of America, "Programable Eletronic Systems (PES) for Use in Safety Applications", Draft 3, ISA-dS84.01, August 1990.

Jones-Lee, M. W., "The value of life. An economic analisys", London, Martin Robertson, 1976

Kuehen, R.E., "Computer redundancy: Design, performance, and the future", IEEE Transactions on Reliability, Vol. R-18, No 1, February 1969, pp. 3-11.

Lees, F.P., "Loss Prevention in the Process Industries", Vol. 2, Butterworths, London, 1980, p.1005.

Lees, F.P., "Loss Prevention in the Process Industries", Volume 1, Butterworths, 1980.

MIL, U.S. Departament of Defense. Military Standardization Handbook: Reliability of Eletronic Equipment MIL-STD-HNBK-217E, 1982.

Mooney, G. H., "The valuation of human life", Mcmillian Publishers, 1977.

NPRD2, Rome Air Development Center, Reliability Analysis Center, "Nonelectronic Parts Reliability Data", Summer 1981.

Oliveira, L.F.S., Frutuoso e Melo, P.F.F., Fleming, P.V., Lima, J.E., e Netto, J.D.A., "Introdução à Análise de Segurança por Árvore de Falhas", Apostila do Curso, COPPE/UFRJ, 1985.

Oliveira, L.F.S., Gamal, H., Simões, S., Faertes, D., "Análise de Confiabilidade do Sistema de Detecção de Incêndio da Zona 21 (Cabeça dos Poços) da Plataforma de Pampo-1", anais do 5º encontro Latino-Americano da Indústrias do Petróleo e Petroquímica, realizado no Rio de Janeiro de 18 a 23 de Outubro de 1992.

Oliveira, L.F.S., Gamal, H., Simões, S., Faertes, D., "Análise de Confiabilidade de Configurações Alternativas de CLPs para Sistemas de Intertravamento e Segurança", anais do III Encontro Técnico sobre Engenharia da Confiabilidade, realizado no Rio de Janeiro de 22 a 24 de Outubro de 1991.

Oliveira, L.F.S., Frutuoso, P.F.F., Gamal, H., "Teoria Cinética de Árvores de Falhas: Uma Versão Simplificada", Apostila do Curso Avançado de Confiabilidade, Junho de 1991.

OREDA Participants, "Offshore Reliability Data", 1ª Edição, 1984.

Rijnmond,"Risk Analisys of Six Potentially Hazardous Industrial Objects in the Rijnmond Area, a Pilot Study - A Report to the Rijnmond Public Authority", p.371-387

SINTEF, Rausand Marvin, "Reliability of Fire & Gas Detector Systems", SINTEF report STF75 A86006, Trondheim, Noruega, 1986.

Vesely, W.E., Goldberg, F.F., Roberts, N.H., e Haasl, D.F., "Fault Tree Handbook", U.S.N.R.C. NUREG-0492, 1981.

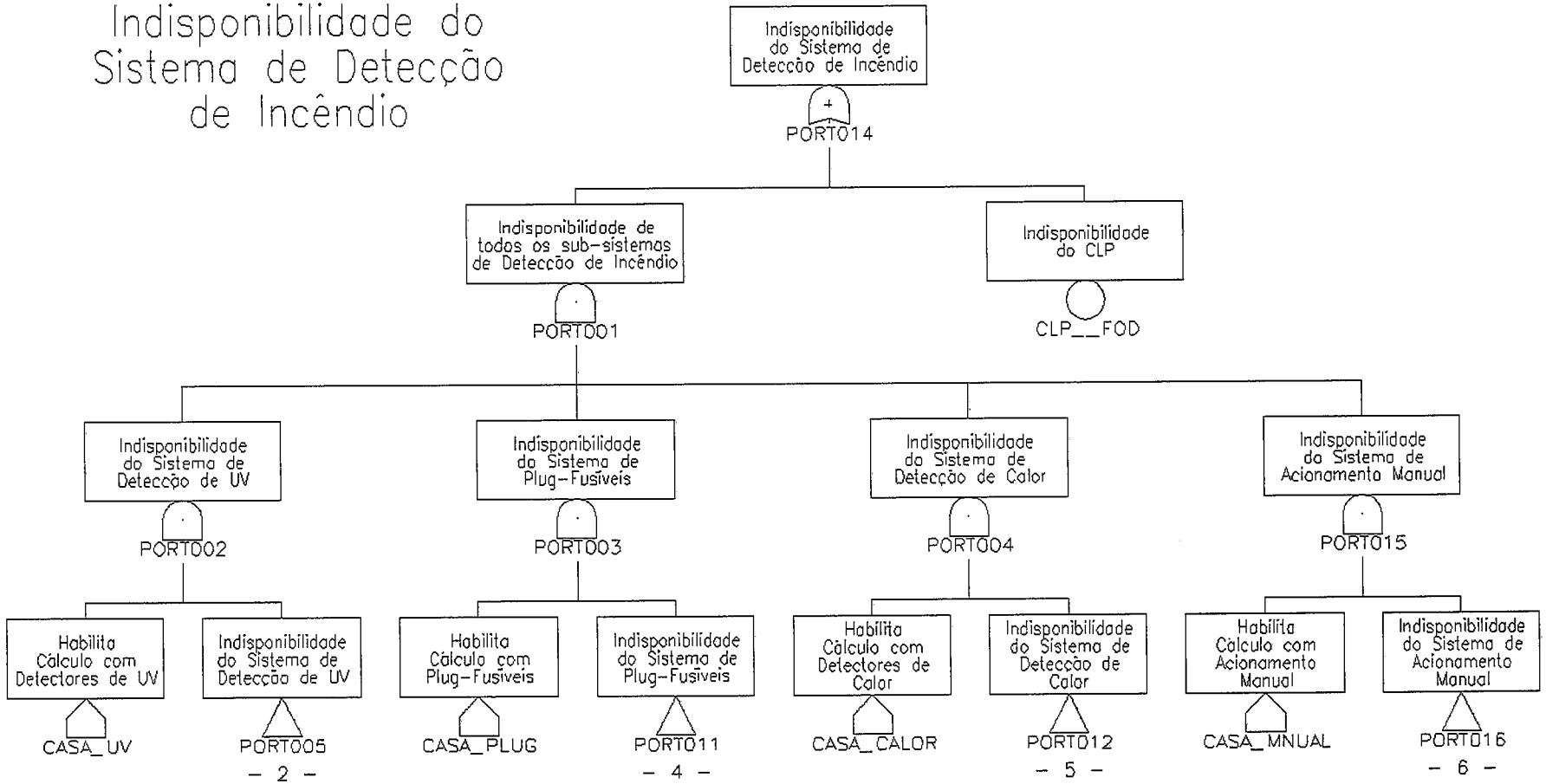
von Neumann, J., "Probabilistic logics and the synthesis of reliable organisms from unreliable components", Automata Studies, Annals of Mathematical Studies, Princeton University Press, No. 34, pp. 43-98, 1956.

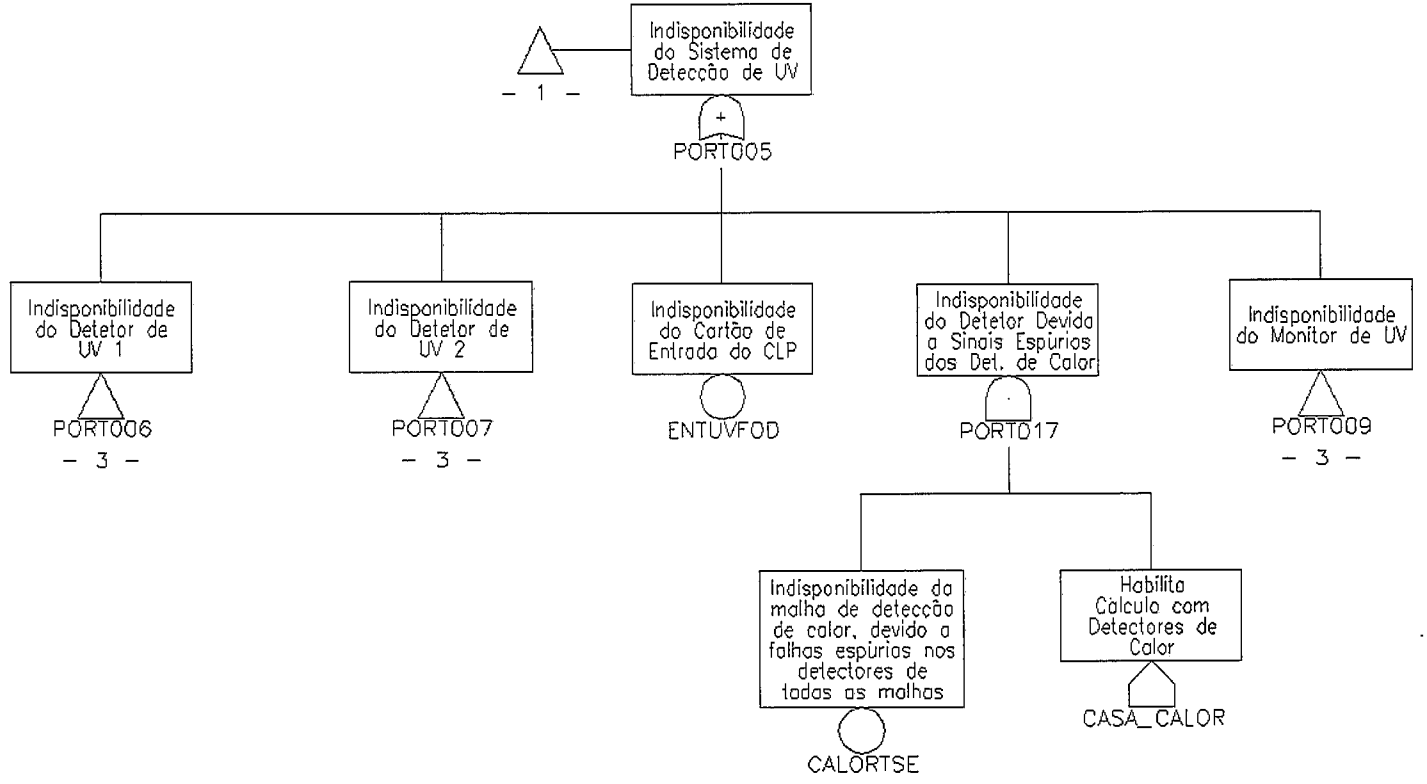
WOAD Statistical Report - "Statistics on Accidents to Offshore Structures Engaged in Oil and Gas Activities in the period 1970-1989", VERITEC - Veritas Offshore Technology and Services A/S, Norway, 1990.

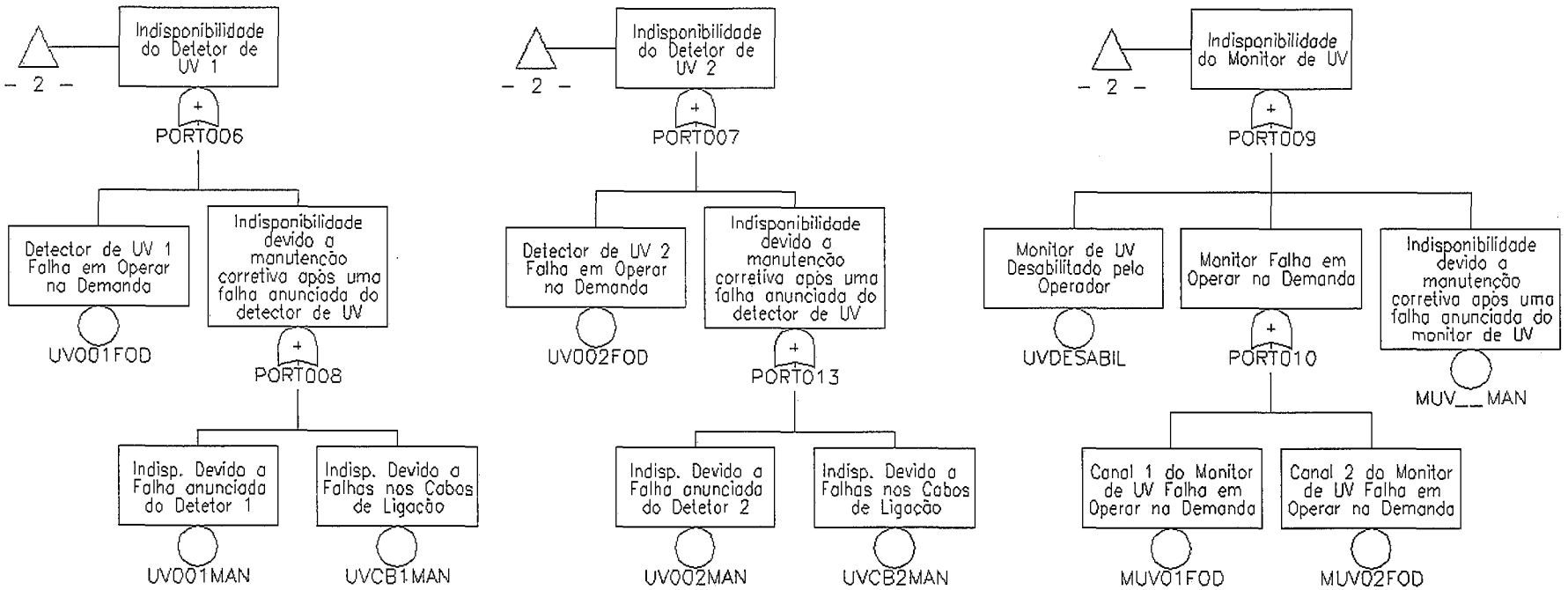
APÊNDICES

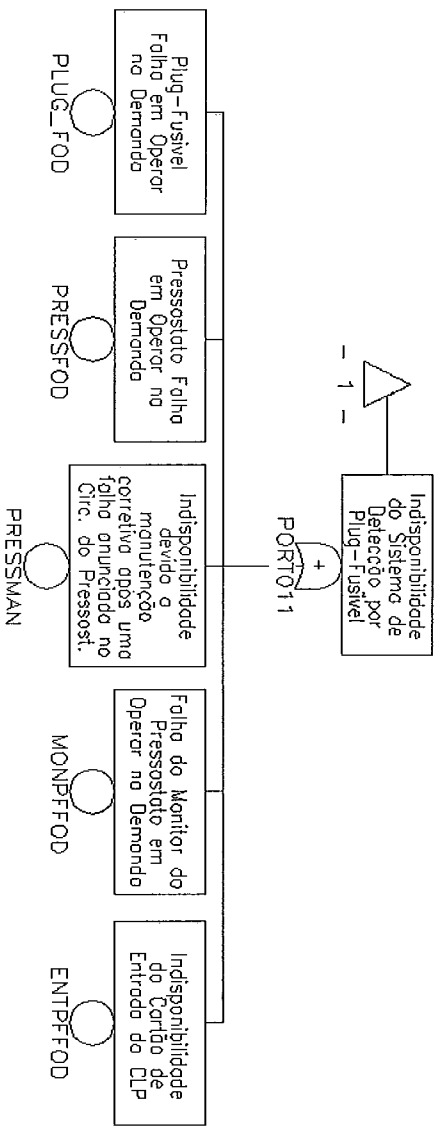
A. Árvore de Falhas de Indisponibilidade

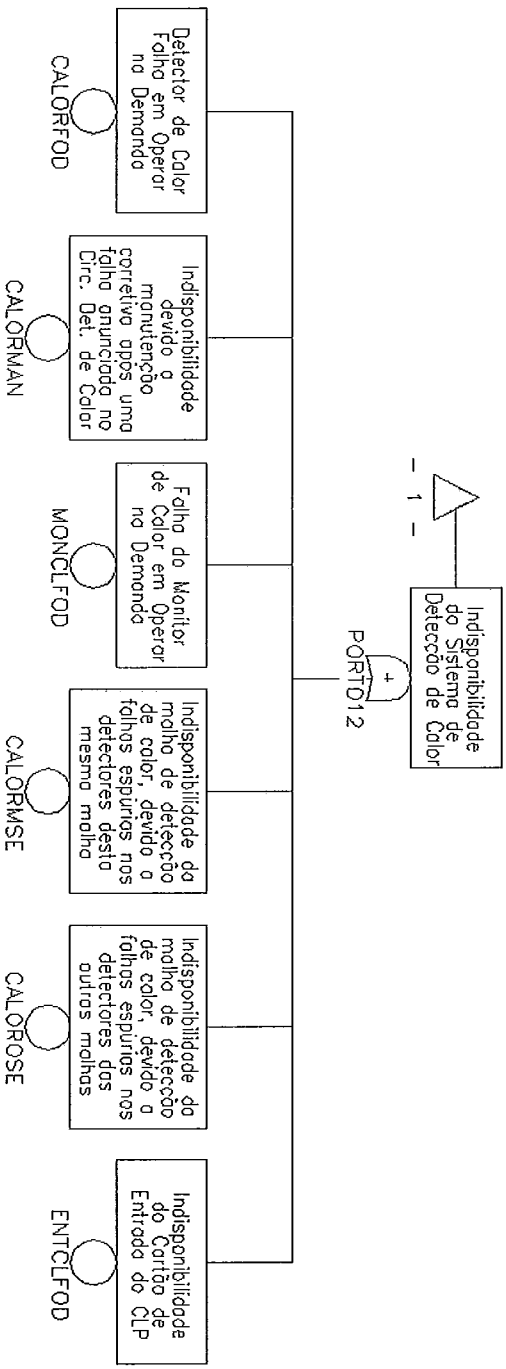
Indisponibilidade do Sistema de Detecção de Incêndio

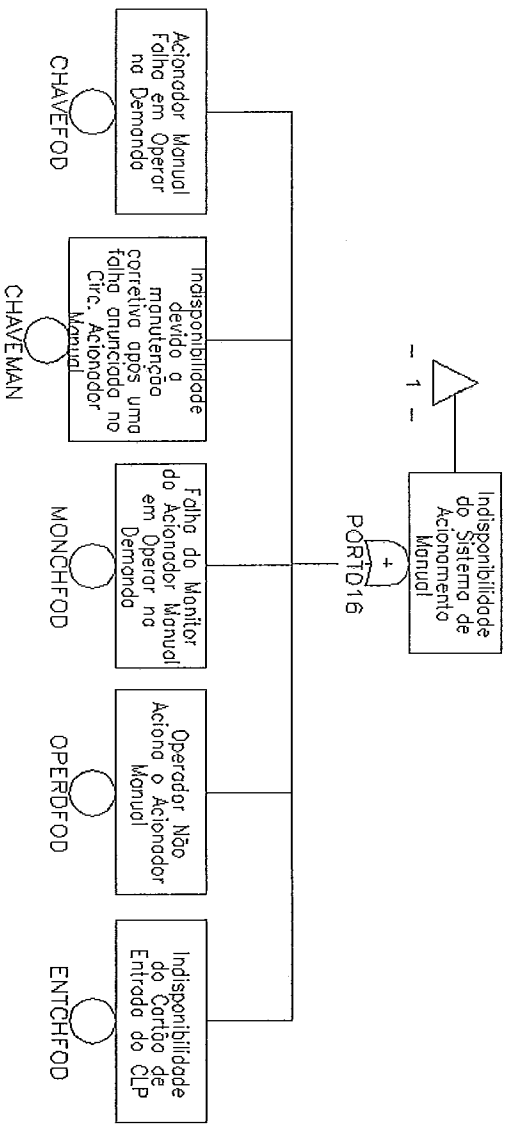



Indisponibilidade do Sistema de Detecção de UV
- 1 -
+
PORT005
Indisponibilidade do Detetor de UV 1
PORT006
- 3 -
Indisponibilidade do Detetor de UV 2
PORT007
- 3 -
Indisponibilidade do Cartão de Entrada do CLP
ENTUVFOD
Indisponibilidade do Detetor Devida a Sinais Espúrios dos Det. de Calor
PORT017
Indisponibilidade do Monitor de UV
PORT009
- 3 -
Indisponibilidade da malha de detecção de calor, devido a falhas espúrias nos detectores de todas as malhas
CALORTSE
Habilita Cálculo com Detectores de Calor
CASA_CALOR


Indisponibilidade do Detetor de UV 1
- 2 -
PORT006
Detector de UV 1 Falha em Operar na Demanda
UV001FOD
Indisponibilidade devido a manutenção corretiva após uma falha anunciada do detector de UV
PORT008
Indisp. Devido a Falha anunciada do Detetor 1
UV001MAN
Indisp. Devido a Falhas nos Cabos de Ligação
UVCB1MAN
Indisponibilidade do Detetor de UV 2
- 2 -
PORT007
Detector de UV 2 Falha em Operar na Demanda
UV002FOD
Indisponibilidade devido a manutenção corretiva após uma falha anunciada do detector de UV
PORT013
Indisp. Devido a Falha anunciada do Detetor 2
UV002MAN
Indisp. Devido a Falhas nos Cabos de Ligação
UVCB2MAN
Indisponibilidade do Monitor de UV
- 2 -
PORT009
Monitor de UV Desabilitado pelo Operador
UVDESABIL
Monitor Falha em Operar na Demanda
PORT010
Indisponibilidade devido a manutenção corretiva após uma falha anunciada do monitor de UV
MUV__MAN
Canal 1 do Monitor de UV Falha em Operar na Demanda
MUV01FOD
Canal 2 do Monitor de UV Falha em Operar na Demanda
MUV02FOD

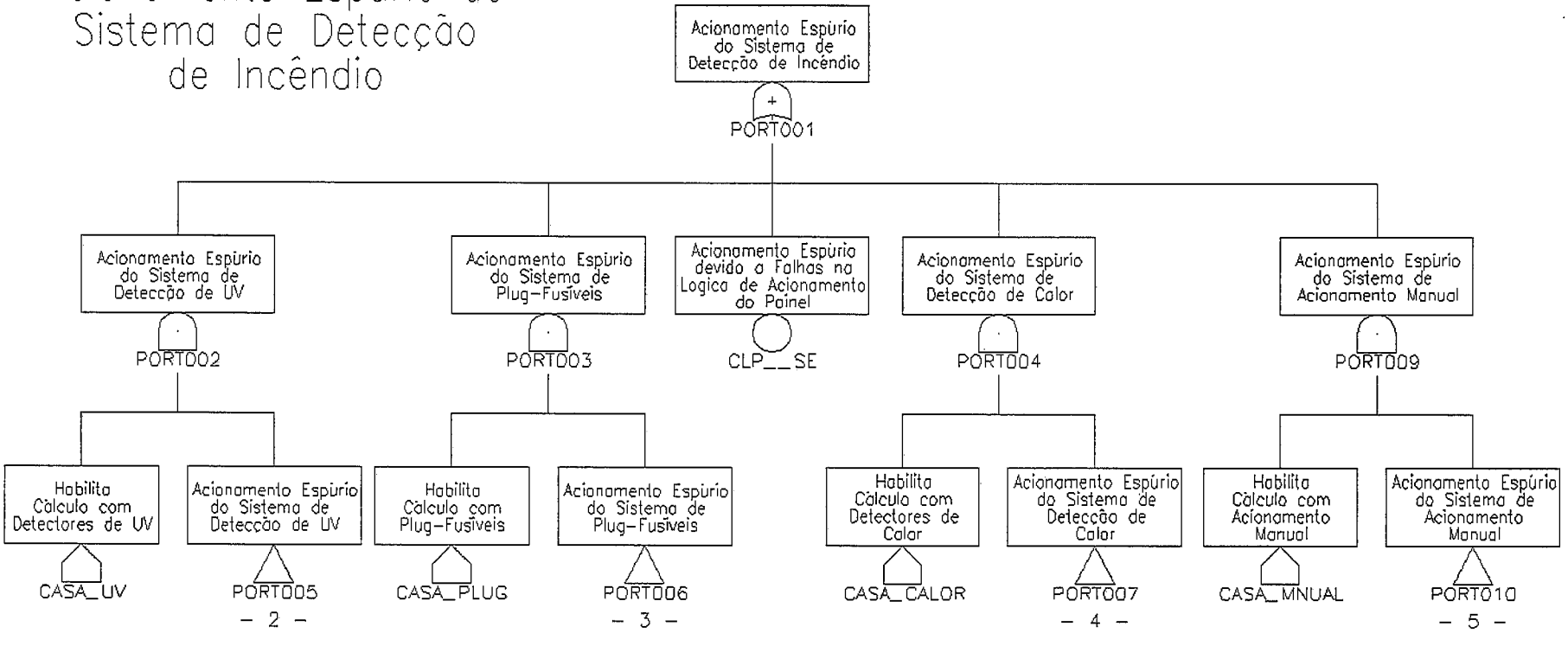

Indisponibilidade do Sistema de Detecção por Plug-Fusível
PORTO11
- 1 -
Plug-Fusível Falha em Operar na Demanda
PLUG_FOD
Pressostato Falha em Operar na Demanda
PRESSFOD
Indisponibilidade devido a manutenção corretiva após uma falha anunciada no Circ. do Pressost.
PRESSMAN
Falha do Monitor do Pressostato em Operar na Demanda
MONPFFOD
Indisponibilidade do Cartão de Entrada do CLP
ENTPFFOD

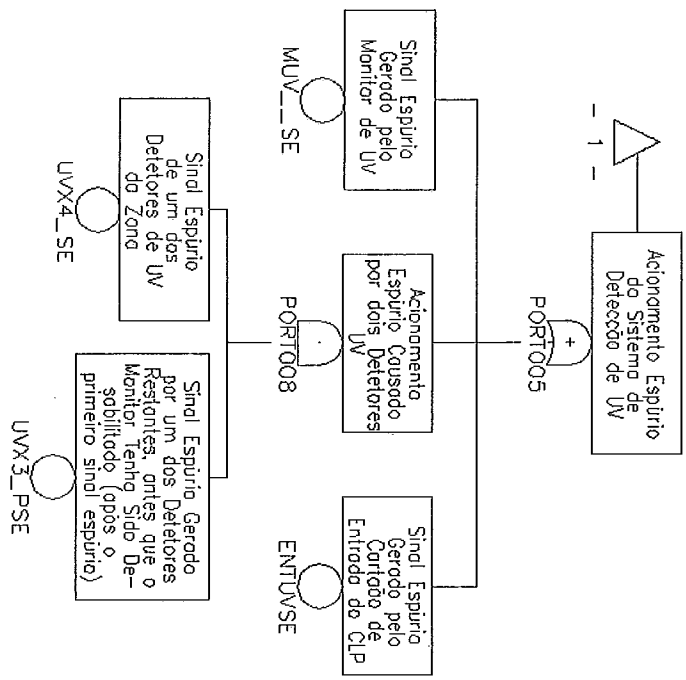

Indisponibilidade do Sistema de Detecção de Calor
PORTO12
- 1 -
Detector de Calor Falha em Operar na Demanda
CALORFOD
Indisponibilidade devido a manutenção corretiva após uma falha anunciada no Circ. Det. de Calor
CALORMAN
Falha do Monitor de Calor em Operar na Demanda
MONCLFOD
Indisponibilidade da malha de detecção de calor, devido a falhas espúrias nos detectores desta mesma malha
CALORMSE
Indisponibilidade da malha de detecção de calor, devido a falhas espúrias nos detectores das outras malhas
CALOROSE
Indisponibilidade do Cartão de Entrada do CLP
ENTCLFOD

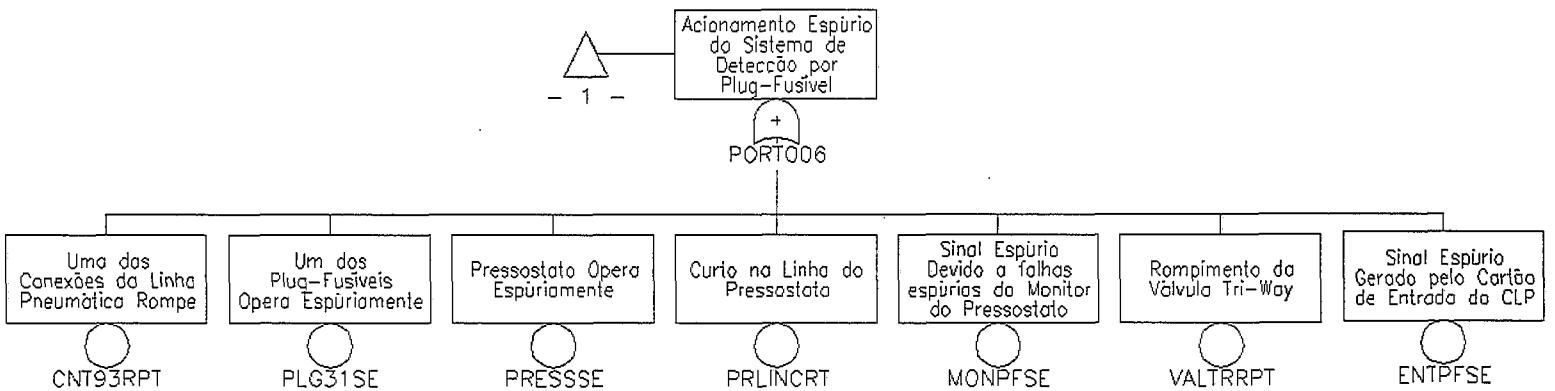

Indisponibilidade do Sistema de Acionamento Manual
PORTD16
Acionador Manual Falha em Operar na Demanda
CHAVEFOD
Indisponibilidade devido a manutenção corretiva após uma falha anunciada no Circ. Acionador Manual
CHAVEMAN
Falha do Monitor do Acionador Manual em Operar na Demanda
MONCHFOD
Operador Não Aciona o Acionador Manual
OPERDFOD
Indisponibilidade do Cartão de Entrada do CLP
ENTCHFOD

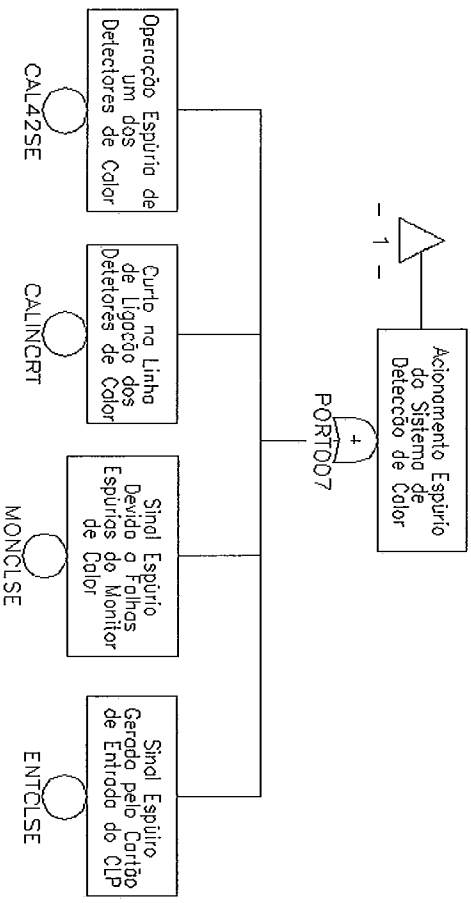
B. Árvore de Falhas de Freqüência Espúria

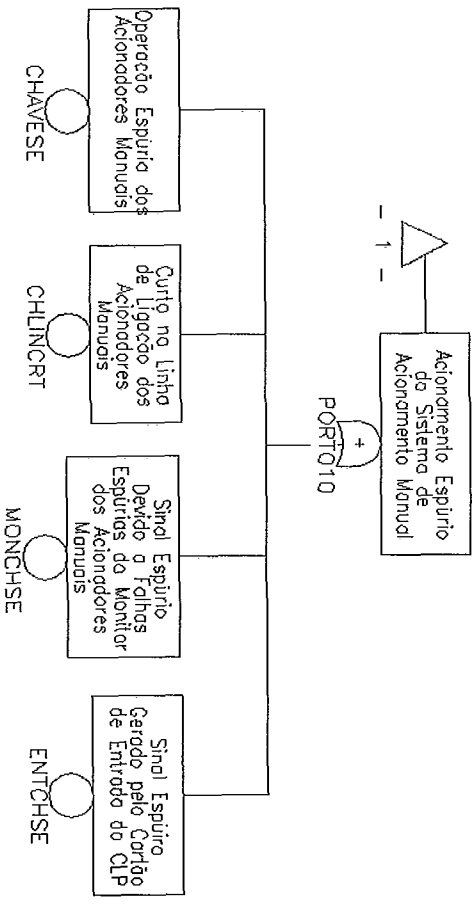
Acionamento Espúrio do Sistema de Detecção de Incêndio




Acionamento Espúrio do Sistema de Detecção de UV
- 1 -
PORT005
Sinal Espúrio Gerado pelo Monitor de UV
MUV__SE
Acionamento Espúrio Causado por dois Detetores UV
PORT008
Sinal Espúrio Gerado pelo Cartão de Entrada do CLP
ENTUVSE
Sinal Espúrio de um dos Detetores de UV da Zona
UVX4_SE
Sinal Espúrio Gerado por um dos Detetores Restantes, antes que o Monitor Tenha Sido Desabilitado (após o primeiro sinal espúrio)
UVX3_PSE


Acionamento Espúrio do Sistema de Detecção por Plug-Fusível
- 1 -
PORTO06
Uma das Conexões da Linha Pneumática Rompe
Um dos Plug-Fusíveis Opera Espúriamente
Pressostato Opera Espúriamente
Curto na Linha do Pressostato
Sinal Espúrio Devido a falhas espúrios do Monitor do Pressostato
Rompimento da Válvula Tri-Way
Sinal Espúrio Gerado pelo Cartão de Entrada do CLP
CNT93RPT
PLG31SE
PRESSSE
PRLINCRT
MONPFSE
VALTRRPT
ENTPFSE


Acionamento Espúrio do Sistema de Detecção de Calor
1
PORT007
Operação Espúria de um dos Detectores de Calor
CAL42SE
Curto na Linha de Ligação dos Detetores de Calor
CALINCRT
Sinal Espúrio Devido a Falhas Espúrias do Monitor de Calor
MONCLSE
Sinal Espúrio Gerado pelo Cartão de Entrada do CLP
ENTCLSE


Acionamento Espúrio do Sistema de Acionamento Manual
1
PORTO10
Operação Espúria dos Acionadores Manuais
Curto na Linha de Ligação dos Acionadores Manuais
Sinal Espúrio Devido a Falhas Espúrias do Monitor dos Acionadores Manuais
Sinal Espúrio Gerado pelo Cartão de Entrada do CLP
CHAVESE
CHLINCRT
MONCHSE
ENTCHSE

C. Planilha Análise Custo-Benefício

Taxa de Juros (anual)	0.080
Vida Util (anos)	20.000

Configuracao atual

Calculo do Custo

Custos do Sistema de Sensoramento

Tipo de Sensor	No. de Sensores	Capital Presente	Capital Anualizado	Manutencao por sensor	Total Anualizado	Custo Total do Sensoramento
UV	8	40,723.62	4147.790	588.66	8857.070	8,857.07
Calor	42	16,770.82	1708.145	146.59	7864.925	7,864.93
P.Fus.	31	32,009.41	3260.229	1.20	3297.429	3,297.43
C. Man.	4	3,173.19	323.197	10.00	363.197	363.20
Custo anualizado total do sensoramento						20,382.62
Custo da configuracao em valor presente						200,119.58

Custos do Sistema de CLP

Configuracao	SIMPLEX	DSIMPLEX	DDUAL 1-2	DDUAL 2-2	TRIPLEX 2-3
Manutencao	1,000.00	1,500.00	2,000.00	2,000.00	3,000.00
Capital Presente	30,000.00	45,000.00	60,000.00	60,000.00	90,000.00
Capital Anualizado	3,055.57	4,583.35	6,111.13	6,111.13	9,166.70
Total	4,055.57	6,083.35	8,111.13	8,111.13	12,166.70
Custo Total do Sistema Anualizado	24,438.19	26,465.97	28,493.75	28,493.75	32,549.32
Custo Total do Sistema em valor Presente	239,937.73	259,846.80	279,755.88	279,755.88	319,574.02

Calculo do Beneficio

Frequencia de incendio na Zona 21 (anual)	1.80E-02
Perda media por incendio (economica)	300,000,000.00
Perda media por incendio (vidas)	0.172
Valor da vida humana	10,000,000.00
Custo da falha espuria	56,688.85
Perda total estimada sem o sistema de detecao (anual)	5,430,960.00

Configuracao	SIMPLEX	DSIMPLEX	DDUAL 1-2	DDUAL 2-2	TRIPLEX 2-3
Indisponibilidade do sistema de detecao	2.74E-02	2.87E-02	3.60E-03	5.40E-02	5.31E-03
Beneficio direto economico anual	5,251,932.00	5,244,912.00	5,380,538.40	5,108,292.00	5,371,304.40
Perda economica residual anual	179,028.00	186,048.00	50,421.60	322,668.00	59,655.60
Beneficio para a seguranca anual	3.01E-03	3.01E-03	3.08E-03	2.93E-03	3.08E-03
Risco residual	8.49E-05	8.89E-05	1.12E-05	1.67E-04	1.65E-05
Beneficio direto anual	5,282,043.08	5,274,982.83	5,411,386.82	5,137,579.54	5,402,099.88
Beneficio direto em valor presente	51,859,877.54	51,790,558.98	53,129,793.48	50,441,513.25	53,038,612.92

Calculo da Reducao do Beneficio devido a Falhas Espurias

Frequencia de falhas espurias (anual)	1.74	1.27	2.75	0.84	0.84
Reducao do beneficio anual dev a falhas esp.	98,638.60	71,994.84	155,894.34	47,618.63	47,618.63

Calculo do Beneficio Liquido

Beneficio liquido	5,183,404.48	5,202,987.99	5,255,492.48	5,089,960.91	5,354,481.24
Beneficio liquido (em relacao a configuraco SIMPLEX)		19,583.51	72,088.00	(93,443.57)	171,076.77

Calculo da Relacao Beneficio/Custo

Relacao beneficio total/custo	212.103	196.592	184.444	178.634	164.504
Dolares gastos/morte estatistica evitada	8.12E+06	8.80E+06	9.24E+06	9.73E+06	1.06E+07

D. Planilha de custo dos subsistemas de sensoramento

Sistema de deteccao de fogo				
Quantidade	Descricao	Preco	Multiplicador	Total
2	Cartao p/ 4 malhas Notifier	826.00	0.625	1,032.50
1	Rack Notifier p/ 16 cartoes	716.00	0.125	89.50
42	Detectores de calor Fenwall	87.00	1	3,654.00
42	Caixas a prova de explosao	10.50	1	441.00
5	Pontos de Logica do painel	82.00	1	410.00
1	Calha	1,010.00	1	1,010.00
83	Prensa cabo 3/4"	15.54	1	1,289.82
250	Metro do fio armada 1 par x 1.5 mm2	2.20	1	550.00
Total				8,476.82
Custo de instalacao				8,294.00
Total incluindo instalacao				16,770.82
Sistema de deteccao de Chama (UV)				
Quantidade	Descricao	Preco		Total
1	Monitor Dettronics para 8 pontos	4,500.00	1	4,500.00
1	Rack para 8 monit. Dettronics	514.37	0.125	64.30
8	Detector de UV CV-7050	1,725.00	1	13,800.00
1	Pontos de Logica do painel	82.00	1	82.00
1	Calha	3,280.00	1	3,280.00
8	Prensa cabo 3/4"	15.54	1	124.32
800	Metro do cabo 1 quadro x 1.5 mm2	4.60	1	3,680.00
Total				25,530.62
Custo de instalacao				15,193.00
Total incluindo instalacao				40,723.62
Sistema de Plug-Fusiveis				
Quantidade	Descricao	Preco		Total
1	Cartao p/ 4 malhas Notifier	826.00	0.25	206.50
1	Rack Notifier p/ 16 cartoes	716.00	0.0625	44.75
31	Plug-Fusiveis	83.30	1	2,582.30
1	Pressostato	1,050.00	1	1,050.00
31	Ts	67.52	1	2,093.12
1	Conj. Reg. de Pressao 3valv+restr+manom.	702	1	702.00
230	Metro de tubo inox 1/4"	22.04	1	5,069.20
1	Pontos de Logica do painel	82.00	1	82.00
1	Calha	3,010.00	1	3,010.00
1	Prensa cabo 3/4"	15.54	1	15.54
100	Cabo armado 1 par de 1.5mm2	2.20	1	220.00
Total				15,075.41
Custo de instalacao				16,934.00
Total incluindo instalacao				32,009.41
Sistema de Acionamento Manual				
Quantidade	Descricao	Preco	Multiplicador	Total
1	Cartao p/ 4 malhas Notifier	826.00	0.625	516.25
1	Rack Notifier p/ 16 cartoes	716.00	0.125	89.50
1	Pontos de Logica do painel	82.00	1	82.00
4	Chaves manuais	30.00	1	120.00
1	Calha	1,010.00	1	1,010.00
1	Prensa cabo 3/4"	15.54	1	15.54
250	Metro do fio armada 1 par x 1.5 mm2	2.20	1	550.00
Total				2,383.29
Custo de instalacao				789.90
Total incluindo instalacao				3,173.19

Custos de Manutencao (por detetor)

Descricao	Custo
Detectores de Calor	146.59
Detectores de UV	588.66
Plug-fusiveis	1.20
Chaves Manuais	10.00

E. Determinação da freqüência de incêndio

E.1. Enfoque clássico

• Nº de ocorrências observadas : 63

Um total de 13 plataformas são especificadas na tabela abaixo, segundo o período de observação de ocorrências (incêndios).

PLATAFORMA	INÍCIO DE COLETA	FIM DE COLETA	TOTAL (MESES)
Enchova	Jan/85	Abril/88	39
Namorado 1	Jan/85	Dez/91	84
Namorado 2	Jan/85	Dez/91	84
Cherne 1	Jan/85	Dez/91	84
Cherne 2	Jan/85	Dez/91	84
Garoupa	Jan/85	Dez/91	84
Pampo	Jan/85	Dez/91	84
Vermelho 1	Jan/88	Dez/91	48
Vermelho 2	Jan/88	Dez/91	48
Vermelho 3	Jan/88	Dez/91	48
Carapeba 1	Jan/88	Dez/91	48
Carapeba 2	Jan/88	Dez/91	48
Pargo	Jan/88	Dez/91	48
Total			831 plat.-meses

• Base Temporal de Observação = (831 ÷ 12) plat.-ano

Considerando Poisson de amostragem censurado no tempo:

• Valor mais provável

$$f_c = \frac{n^o \text{ de inc.}}{B} = \frac{63}{831} \times 12 \ ,$$

onde B é a base temporal de observação.

$$f_c = 0{,}91 \ \textit{inc./plat.-ano}$$

• Limite inferior (5% de confiança)

r = nº de incêndios = 63

n = graus de liberdade = 2r = 126

B = base temporal de observação = 831/12 plat.-ano

$\chi^2_{2r\,:\,0{,}05} = 101{,}08$

$$f_{LI} = \frac{\chi^2_{2r\,:\,0{,}05}}{2 \times B} = \frac{\chi^2_{126\,:\,0{,}05}}{2 \times (831 \div 12)}$$

$$f_{LI} = 0{,}73 \ \textit{inc./plat.-ano}$$

• Limite Superior (95% de confiança)

r = nº de incêndios = 63

n = graus de liberdade = 2r = 126

B = base temporal de observação = 831/12 plat.-ano

$\chi^2_{2r+2:}$ =155,4

$$f_{LS} = \frac{\chi^2_{2r+2:\,0,95}}{2 \times B} = \frac{\chi^2_{128:\,0,95}}{2 \times (831 \div 12)}$$

$$f_{LS} = 1,12 \; inc./plat.-ano$$

• Freqüência de incêndio por zona (anual) = f

f = 0,91 inc./ plat-ano ÷ 50

f = 1,82 E-2

E.2. Enfoque bayesiano

Segundo WOAD (1990), em plataformas fixas, tem-se:

$$f = 2,8 \times 10^{-3} \; inc./plat.-ano$$

Admitindo que este é apenas o limite inferior (percentil 5%, devido a "under-reporting"), que o limite superior x_{95} seria 100 vezes maior que este e que esta incerteza pode ser descrita por uma distribuição lognormal, então:

Distribuição a priori, lognormal com $x_5 = 2{,}8 \cdot 10^{-3}$ e $x_{95} = 2{,}8 \cdot 10^{-1}$

$$FE = \sqrt{(x_{95} \div x_5)} = 10$$

- Distribuição de verossimilhança

Poisson com:

$$\lambda = \frac{63 \ observações}{(831 \div 12) \ plat.-anos} = 0{,}91 \ inc./plat.-anos$$

Parâmetros de distribuição a posteriori são apresentados a seguir.

$$\mu = 0{,}86 \ inc./plat.-anos$$

$$\sigma^2 = 2{,}07 \cdot 10^{-3}$$

F. Determinação das perdas devido a incêndio e falhas espúrias

F.1. Perdas humanas por incêndio

Segundo o WOAD (1990), no período de 1970 à 1989 nos 145 acidentes registrados ocorreram um total de 25 mortes, resultando uma média de mortes por incêndio neste período de 17.2%.

F.2. Perdas econômicas por incêndio

Na avaliação da perda média por incêndio foram considerados incêndios que causam avarias severas à estrutura da plataforma ou perda totais da unidade (perdas totais sobre o ponto de vista de corretora de seguros). Admitindo-se que a plataforma após este tipo de incêndio fica inoperante, é necessário computar-se também as perdas devidas a perda de produção durante o período de reparo da unidade. Neste trabalho o período médio inatividade considerado foi de 10 meses.

Admitindo-se uma perda de produção diária de cerca de US$ 560.000,00 de óleo e US$ 32.000,00 de gás, obtem-se um prejuízo de aproximadamente US$ 600.000,00 por dia ou US$ 180.000.000,00 no período de 10 meses.

Segundo o WOAD (1990), no período de 1970 a 1989, ocorreram:

- 31 perdas totais de unidades - custo estimado (pelo grupo de trabalho) de cerca de US$ 300.000.000,00; e

- 62 ocorrências de danos severos à estrutura - custo estimado de US$ 50.000.000.00.

A média obtida a partir dos dados acima implica em um custo médio de reparo da plataforma após um incêndio de aproximadamente US$ 120.000.000,00.

Somando-se as componentes da perda média de produção com o custo médio de reparo após um incêndio, causador de danos estruturais severos

à estrutura ou perda total da unidade, obtem-se um prejuízo total de aproximadamente US$ 300.000.000,00 por incêndio.

F.2. Perdas econômicas por falha espúria

Segundo informações de especialistas a parada de produção por falha espúria ocasiona:

- 500 m^3 de óleo não produzido

- 30.000 m^3 de gás não produzido

- 120.000 m^3 de gás queimado

Cálculo do custo por parada espúria:

a) Óleo (C_1)

- preço do óleo: US$ 14.13 / bbl

C_1 = 500 m^3 x 6,29 bbl/m^3 x 14.13 US$/bbl = US$ 44,438.85

b) Gás (C_2)

- preço do gás = US$ 83 /1000 m_3

C_2 = (30.000 + 120.000) m^3 x US$ 83 / 1000 m^3 = US$ 12,450.00

Custo de Falha Espúria = US$ 56,888.85