ESTUDO DA DISPONIBILIDADE DE UM CENTRO DE SUPERVISÃO BASEADO EM UMA ARQUITETURA DISTRIBUIDA

Homero Gonçalves de Andrade

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

Aprovada por:

Sueli Mendes dos Santos
(Presidente)

Antonio Luiz Bogado Fernandes

Jorge Moreira de Souza

Edil Severiano Tavares Fernandes

RIO DE JANEIRO, RJ - BRASIL
FEVEREIRO DE 1983

ANDRADE, HOMERO GONÇALVES DE

Avaliação da Disponibilidade de um Centro de Supervisão Baseado em uma Arquitetura Distribuída (Rio de Janeiro) 1983.

X,171p, 29,7cm (COPPE-UFRJ, M.Sc., Engenharia de Sistemas e Computação, 1983).

Tese - Universidade Federal do Rio de Janeiro, CEPEL.

1. Avaliação de Disponibilidade.

I. COPPE/UFRJ II. Título (série)

Agradeço à direção do Centro de Pesquisas de Energia Elétrica - CEPEL, pela oportunidade de realização do presente trabalho.

Aos meus colegas e amigos do Departamento de Eletrônica do CEPEL e aos engenheiros de FURNAS, agradeço pela participação no projeto que originou este trabalho de tese.

Aos colegas da Área de Centros de Supervisão do Departamento de Eletrônica do CEPEL, Maurício Moszkowicz e Lúcia Della Valle pela colaboração prestada.

A Antônio Luiz Bogado Fernandes pela coordenação do trabalho.

Agradeço especialmente a minha família o incentivo e compreenção pela redução de meu tempo no convívio com eles, para que este trabalho pudesse ser realizado.

Ao corpo de datilógrafas do Departamento de Eletrônica, em especial à Angela de Melo Machado.

SINOPSE

O objetivo deste trabalho é apresentar um estudo relativo à introdução de técnicas de tolerância a falhas numa rede local de microprocessadores, construída com a finalidade de realizar as funções de um Centro de Supervisão e Controle para sistemas elétricos.

Os temas abordados neste trabalho são:

i - apresentação das principais técnicas existentes na literatura para tornar um sistema tolerante a falhas;

ii - estudo do sistema no qual se deseja introduzir técnicas de tolerância a falhas;

iii - desenvolvimento de técnicas de detecção e recuperação de falhas transientes e permanentes;

iv - modelagem do sistema com o objetivo de avaliar a disponibilidade deste, após a introdução das técnicas de tolerância a falhas;

v - desenvolvimento de um sistema para testar a eficiência das técnicas propostas.

As técnicas de tolerância a falhas transientes propostas mostraram-se extremamente eficientes, ficando a disponibilidade do sistema, após a aplicação das técnicas, praticamente independente das falhas transientes.

ABSTRACT

The purpose of this work is to present a study about fault-tolerance technics introduced in a Supervisory and Control Dispatch Center for electrical power systems built around a local network of microprocessors.

The main topics described are:

i - an overview of the main fault-tolerant technics found in the litterature;

ii - a study of the system to which we wanted to apply fault-tolerance technics;

iii - development of hardware and software methods to detect and recover transient and permannent faults;

iv - a method for the evaluation of a system availability, after the introduction of fault-tolerance technics;

v - development of a measuring method to find the numerical values of the parameters needed by the method above.

The proposed transient fault-tolerance technics proved to be very efficient, and the resulting system availability turned out to be independent of transient faults.

INDICE

CAPÍTULO I

INTRODUÇÃO

O estudo de computadores tolerantes a falhas é uma disciplina rigorosa que abrange desde o projeto, a análise e a manutenção de sistemas altamente confiáveis (1).

Logo que os computadores começaram a ser usados em larga escala em todos os setores, sentiu-se a necessidade da introdução de técnicas que os tornassem tolerantes a falhas. Em determinadas aplicações, uma falha pode colocar em perigo vidas humanas ou provocar grandes prejuízos econômicos. No caso dos centros de supervisão e controle para sistemas elétricos exige-se um alto grau de confiabilidade, pois uma pane ou uma operação indevida da rede elétrica pode provocar danos incalculáveis.

O estudo da confiabilidade obteve um grande impulso no início dos anos sessenta, no programa espacial. Isto explica o grande número de trabalhos na área de sistemas fechados (sem manutenção), altamente confiáveis. Este campo evoluiu e passou a abranger um vasto campo de problemas relacionados com a confiabilidade de sistemas de computadores, empregados em atividades industriais em geral.

O trabalho aqui apresentado, entretanto, refere-se ao estudo de um subconjunto destes problemas que são os relacionados a sistemas que admitem manutenção (sistemas reparáveis). As técnicas estudadas visarão o aumento da confiabilidade de uma rede local de microprocessadores, que será usada para construir um centro de supervisão e controle de sistemas de geração, transmissão e distribuição de energia elétrica. As principais características destes centros que interessam ao estudo da confiabilidade, são:

i - O sistema admite manutenção;
ii - É um sistema para controle em malha aberta (a decisão final é do operador humano);
iii - Apresenta apenas alguns pontos vitais;
iv - Permite operação em modo degradado;
v - Existe uma grande redundância nas informações apresentadas aos operadores;
vi - O sistema é distribuído;
vii - Os operadores do sistema elétrico (despachantes) conhecem perfeitamente o sistema sob controle.

Neste trabalho não criamos mais teorias e modelos na já tão vasta e rica literatura desta área. Procuramos usar os conceitos, métodos, modelos e sugestões existentes, fazendo apenas pequenas alterações para adaptá-los à nossa aplicação. Assim sendo, na parte de modelagem aplicamos o modelo desenvolvido por Ying W. Ng (1). Observamos que os trabalhos nesta área geralmente dão pouca ênfase ao estudo das falhas transientes e muitos deles usam parâmetros nos modelos que são difíceis de serem estimados. Ying W. Ng procurou unificar os vários tipos de sistema encontrados e trata as falhas transientes e permanentes de uma forma homogênea. Com relação ao desenvolvimento geral do trabalho , procuramos seguir uma metodologia proposta por A. Avizienis adaptando-a à nossa aplicação (2,3).

Acreditamos que a principal contribuição deste trabalho está nas técnicas de detecção e recuperação propostas e no sistema desenvolvido para medir a eficiência (cobertura) das técnicas de tolerância a falhas propostas, principalmente no tocante às falhas transientes, já que pouca coisa se encontra a respeito na literatura existente.

No capítulo II será feita uma breve revisão dos principais conceitos, definições e técnicas normalmente usadas em confiabilidade.

No capítulo III apresentaremos o sistema desenvolvido pelo CEPEL, para supervisão e controle de sistemas elétricos.

Mostramos ainda a necessidade de melhorar a disponibilidade deste sistema para atingir os índices exigidos pelas empresas do setor.

No capítulo IV, seguindo a metodologia de projeto adotada, faremos a identificação e a caracterização do conjunto de falhas que se deseja tolerar. Neste capítulo será proposto ainda um conjunto de técnicas para detecção e recuperação dos diversos tipos de falhas. Proporemos ainda um mecanismo de observação do sistema que será útil na medição do desempenho do sistema e na coleta de dados para estudos futuros.

No capítulo V faremos uma modelagem do sistema completo, com todas as técnicas propostas incorporadas ao sistema. Neste ponto sentiremos a necessidade de algumas ferramentas para avaliação de alguns parâmetros do modelo.

O capítulo VI descreve o sistema desenvolvido para medir a eficiência das técnicas propostas e mostra o desempenho das técnicas de recuperação propostas, na presença de uma falha transiente.

CAPÍTULO II

CONCEITOS BÁSICOS

II.1 INTRODUÇÃO

Neste capítulo faremos uma apresentação das principais definições, conceitos e técnicas usadas em tolerância a falhas.

Inicialmente definiremos os principais termos usados tais como: falha, erro e pane. Em seguida, faremos uma breve apresentação das principais características de uma falha. Para completar a terminologia usada mostraremos as definições, formais e informais, das duas grandezas (confiabilidade e disponibilidade) usadas neste trabalho para avaliar a qualidade de um sistema.

Continuando, mostraremos as principais estratégias para tornar um sistema confiável: intolerância, tolerância a falhas e degradação do desempenho. Os sistemas tolerantes a falhas serão apresentados com o objetivo de situar o nosso projeto dentro desta classificação.

Descreveremos os três tipos de técnicas que são introduzidas em um sistema para torná-lo tolerante a falhas (redundâncias de "hardware","software" e de tempo). Para as redundâncias de "hardware" mostraremos as estáticas e dinâmicas.

Concluindo o capítulo, apresentaremos a metodologia adotada no desenvolvimento do restante deste trabalho.

II.2 DEFINIÇÕES DE FALHA, ERRO E PANE (1,2,3,4)

FALHA é uma mudança não especificada em uma ou mais variáveis lógicas no "hardware" do sistema. Uma falha pode

produzir um ERRO que é o desvio da máquina lógica do seu comportamento especificado, ou seja, o erro é a manifestação de uma falha. Exemplificando, uma falha pode ser um "bit" de memória que fique permanentemente em um mesmo valor lógico. Esta falha pode provocar um erro como a execução errada de uma instrução, uma operação aritmética errada, etc.

Uma falha física é aquela que foi produzida por um evento físico como o mau funcionamento de um componente de "hardware", ou por interferência do meio onde se encontra instalado o sistema. Uma falha não física é aquela produzida por um evento não físico como um erro de projeto, montagem ou por um mau uso do sistema pelos operadores.

Devemos ter cuidado em distingüir erro de falha; uma falha pode ou não produzir um erro, dependendo do estado do sistema. Um erro implica sempre na existência de uma falha, entretanto, a recíproca não é sempre verdadeira. Um mesmo erro pode ser provocado por várias falhas diferentes, enquanto uma única falha pode provocar diferentes erros. Uma falha latente é aquela que não provoca um erro. Como exemplo podemos citar o caso de um "flip-flop", que armazena a condição de "overflow" numa unidade aritmética de um computador, que esteja permanentemente em zero. O erro só será produzido quando realmente ocorrer uma condição de "overflow" durante uma operação aritmética. Assim a falha fica latente até que haja uma solicitação.

Uma falha (ou um erro) é dita PERMANENTE quando ela é contínua e estável (refletindo uma mudança irreversível no "hardware"), TRANSIENTE se ela for de duração limitada, tendo sido causada por um mau funcionamento temporário de um componente ou por interferência externa. As falhas transientes que ocorrem repetidas vezes são ditas INTERMITENTES.

Um sistema estará no estado de PANE quando ele deixar de executar pelo menos uma função no processamento de uma informação.

II.3 CARACTERIZAÇÃO DE UMA FALHA FÍSICA (2,3)

As definições de falha, erro e pane, feitas anteriormente, partiram da hipótese de que o sistema estava funcionando corretamente quando da ocorrência de uma falha. Consideramos como um postulado que as falhas de projeto, tanto de "hardware" como "software", foram previamente eliminadas.

Durante a execução de um programa, o "hardware" de uma máquina pode ser afetado por uma falha que pode ter sido produzida por três tipos de eventos distintos: um dano permanente de algum componente de "hardware", um mau funcionamento temporário de algum elemento ou uma interferência externa.

Existem três parâmetros úteis na classificação de uma falha: tempo de duração, extensão e valor.

A caracterização de uma falha deve incluir o tempo máximo de duração desta falha. Uma falha cuja ocorrência no tempo exceda este parâmetro será interpretada como sendo uma falha permanente pelos mecanismos de recuperação. Caso contrário será tida como transiente. Neste caso são importantes também a taxa de chegada e o tempo médio de duração destas falhas.

A classificação de uma falha quanto ao valor e extensão é aplicada para falhas permanentes e transientes.

A extensão de uma falha indica o número de variáveis lógicas afetadas quando da ocorrência da falha. Uma falha é local (simples) quando ela afeta somente uma variável, enquanto a distribuída afeta mais de uma variável ou até todo o sistema. A proximidade física dos elementos lógicos dos circuitos da nova geração (MSI e LSI), tornaram as falhas distribuídas muito mais comuns (1). As falhas distribuídas são principalmente aquelas geradas por elementos críticos: relógio, fonte de alimentação, barramento de dados, etc.

Com relação ao valor, uma falha pode ser: determinada, quando a variável afetada assume um valor fixo ou indeterminada, quando o valor assumido pela variável durante o período que perdurar a falha for variável.

É importante notar que o conceito de extensão e valor de uma falha aplica-se exclusivamente ao ponto onde ela ocorreu, pois os erros produzidos por esta falha podem se alastrar pelo sistema, produzindo diversos sintomas relativos àquela falha.

II.4 DEFINIÇÃO DAS GRANDEZAS USADAS

As principais grandezas usadas para medir o desempenho de um sistema em relação a tolerância a falhas são:

Confiabilidade - é a probabilidade do sistema operar corretamente até o instante de tempo t = T, dado que ele estava operando em t = 0;

Disponibilidade - é a probabilidade do sistema estar pronto para operar corretamente, no instante t = T;

De uma maneira bem geral, podemos dizer que um sistema pode se encontrar em seis diferentes macro-estados (ver figura II.1) (5):

1 - As tarefas estão sendo executadas corretamente;
2 - O sistema não está sendo solicitado, mas pode executar suas tarefas corretamente;
3 - Ocorreu uma falha não catastrófica durante a execução de uma tarefa;
4 - A demanda de execução possibilita o aparecimento de uma falha não catastrófica;
5 - Uma falha catastrófica apareceu durante a execução de uma tarefa;
6 - A demanda de execução possibilita o aparecimento de uma falha catastrófica.

FC _ FALHA CATASTRÓFICA,
FNC _ FALHA NÃO CATASTRÓFICA
MP _ MANUTENÇÃO PREVENTIVA
MC _ MANUTENÇÃO CORRETIVA

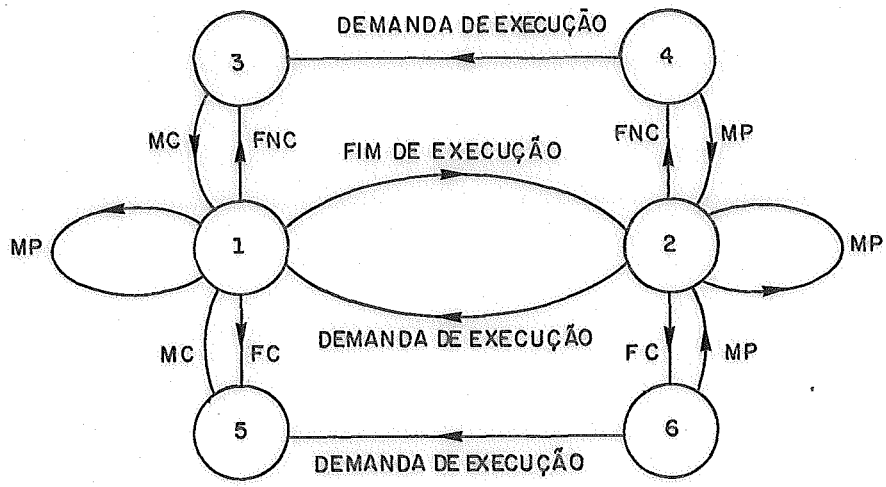


FIGURA (II.1) POSSÍVEIS ESTADOS DE UM SISTEMA

CONFIABILIDADE	$R(t) = P\left[\underline{z}(\tau) = \{1,2\},\ \forall \tau \in [0,t]\right]$
DISPONIBILIDADE	$A(t) = P\left[\underline{z}(t) = \{1,2\}\ \underline{z}(\tau) = \{1,2,3,4,5,6\}, \forall \tau \in [0,t)\right]$
DISPONIBILIDADE ESTACIONÁRIA	$A = \lim_{t \to \infty} A(t)$

TABELA (II.1)

P(X) PROBABILIDADE DE QUE O EVENTO OCORRA

$\underline{z}(t) = i$ FUNÇÃO QUE INDICA QUE O SISTEMA ESTÁ NO ESTADO i NO INSTANTE DE TEMPO t

A partir destes macro-estados assim definidos (5), podemos dar definições precisas para as grandezas normalmente usadas no estudo de sistemas tolerantes a falhas (ver tabela II.1).

O parâmetro confiabilidade é mais usado para sistemas fechados, que têm um determinado tempo de missão e se deseja medir a probabilidade do sistema cumprir esta missão, não levando em conta se o sistema admite manutenção manual (6).

Para nossa aplicação onde o equipamento deve ter uma vida útil de mais de dez anos, e o sistema é acessível à manutenção com tempos de reparo não muito grandes, a disponibilidade estacionária é o parâmetro mais útil, pois mostra a probabilidade do sistema estar operando em t, quando t tende para infinito, mesmo que tenham ocorrido algumas falhas anteriormente.

Deste ponto em diante adotaremos o parâmetro disponibilidade estacionária para medir a qualidade do sistema em relação a tolerância a falhas. Também usaremos apenas o termo disponibilidade para nos referirmos à disponibilidade estacionária.

II.5 TOLERÂNCIA A FALHAS (1,2,3,4)

São duas as principais estratégias usadas para tornar um sistema de computador confiável. Estas estratégias podem ser aplicadas em todos os níveis de um sistema, podendo ser aplicados em elementos de "hardware", programas, microprogramas, base de dados, etc.

A primeira estratégia a ser empregada foi a chamada intolerância a falhas que consiste na eliminação da causa, ou seja, às falhas do sistema. Este objetivo é conseguido usando-se por exemplo, no caso do "hardware", componentes de altíssima qualidade, cuidadosamente escolhidos, rigorosamente testados e empregando-se sofisticadas técnicas de montagem.

Neste método não se empregam redundâncias, todo o esforço é despendido no sentido de melhorar a qualidade do sistema. Na prática, não se pode garantir que a fonte de falhas do sistema seja eliminada. Procura-se apenas reduzí-la ao máximo através do projeto e construção de sistemas de alta qualidade.

A estratégia de intolerância a falhas, tradicionalmente a mais empregada, mostrou-se insuficiente nos seguintes casos (3):

i - Sistemas que não admitem interrupção de seu funcionamento;

ii - Sistemas cujo o MTBF deve ser maior do que se pode obter com a tecnologia atual;

iii - Sistemas onde a paralisação do processamento e/ou realização de manutenção apresentam custo elevado.

Uma alternativa ao método da intolerância a falhas seria a tolerância a falhas. Neste caso a confiabilidade do sistema é obtida pelo emprego de redundâncias.

A definição mais amplamente aceita de um sistema tolerante a falhas é a de sistemas capazes de manter a execução correta dos programas e funções de entrada e saída, mesmo na presença de uma falha pertencente a um conjunto previamente determinado (3).

A tolerância a falhas é um atributo que difere fundamentalmente dos outros atributos de uma máquina, pois os mecanismos que são adicionados a um sistema com esta finalidade podem parecer supérfluos na ausência de uma falha no sistema. Além de muitas vezes implicarem em redução do desempenho, acarretam um custo adicional tanto de "software" quanto de "hardware". Entretanto, são tais mecanismos que poderão garantir a continuidade de funcionamento do sistema na presença de uma falha. Na verdade, estes mecanismos devem ser considerados desde as fases iniciais de projetos corretamente

conduzidos (4).

Nesta filosofia aceita-se que a falha apareça e induza um erro, que é automaticamente eliminado pela redundância. As partes redundantes permanecem em uma condição de sobressalentes, prontas para manter o processamento em caso de ocorrência de uma falha. Este método difere da intolerância a falhas, pois nesta, a equipe de manutenção é invocada logo após a interrupção do processamento, provocando a parada do sistema durante o período de manutenção. No processamento com tolerância a falhas a manutenção das partes do sistema com falha é aceitável simultaneamente à execução correta dos programas (sistemas onde é possível a manutenção manual).

Dizemos que um sistema tolerante a falhas está em estado de pane quando ocorre uma falha que deveria ter sido tolerada, mas os mecanismos de proteção contra falhas não atingiram sua meta, ou então porque esgotaram-se os recursos. Neste caso haverá necessidade de intervenção externa, interrompendo-se o processamento normal. Rigorosamente falando, um sistema é tolerante a falhas somente se nenhuma assistência externa for exigida para implementação deste atributo. Entretanto, a maioria dos computadores da atual geração embora precisando de assistência manual, empregam técnicas de tolerância a falhas como: auto-diagnóstico, paridade na memória, "watch-dog" que são úteis para melhorar o desempenho do sistema.

Um sistema é chamado parcialmente tolerante a falhas (ou levemente degradável) se ele tem a capacidade de reduzir sua capacidade de processamento, reconfigurando-se para um sistema de menor porte, descartando algumas funções ou aumentando o tempo de execução de seus programas. Esta redução deve-se a uma mudança na configuração do sistema devido a uma falha de "hardware" ou "software" (3).

O principal argumento contra o uso de técnicas de tolerância a falhas em um sistema de computadores, está no custo de se colocar redundâncias. Entretanto, a evolução tecnológica dos componentes, a redução do custo de fabricação

de elementos de "hardware", o alto custo do "software" para testes e aumento nos requisitos de confiabilidade deverão incentivar cada vez mais o uso de técnicas de tolerância a falhas.

Concluindo, a experiência e análise dos dois métodos mostraram que o uso dos dois em conjunto dão origem a sistemas altamente confiáveis. A tolerância a falhas, por si só, não elimina a necessidade do uso de técnicas e componentes de boa qualidade. Por outro lado, estes não garantem a confiabilidade ou disponibilidade exigidas por alguns sistemas, ou mesmo que garantam, sem as técnicas de tolerância a falhas, os custos podem ser muito elevados.

II.6 CLASSIFICAÇÃO DOS SISTEMAS TOLERANTES A FALHAS (3)

Podemos distingüir dois tipos fundamentais de sistemas tolerantes a falhas:

i - Sistemas completamente tolerantes a falhas;

ii - Sistemas manualmente controlados com técnicas de tolerância a falhas.

O primeiro completa todas as ações necessárias à recuperação do sistema sem intervenção humana. No segundo a decisão do homem faz parte do procedimento de recuperação. Esta decisão pode ser tomada em diversos estágios do procedimento de recuperação tais como: execução de um programa de diagnóstico, reinicialização do sistema, acionamento de uma chave para desconectar uma parte defeituosa, etc.

Os sistemas completamente tolerantes a falhas ainda podem ser sub-divididos em função da possibilidade de manutenção externa das partes defeituosas.

Nos sistemas fechados não é permitido que haja manutenção manual das partes defeituosas, e o sistema entrará em estado de pane quando se esgotarem todos os recursos de redundância. Os

sistemas fechados são freqüentemente encontrados em aplicação dentro de veículos espaciais.

Nos sistemas reparáveis as partes defeituosas são automaticamente identificadas, isoladas e substituídas, ficando os módulos defeituosos disponíveis para manutenção. Um sistema reparável entra em estado de pane geralmente por imperfeição nos algoritmos de detecção e recuperação, por uma falha catastrófica (é uma falha que produz tantos danos ao sistema, que torna a recuperação deste impossível) ou se ocorrerem falhas numa taxa maior que a taxa de manutenção.

O sistema que será tratado neste trabalho a título de exemplo e que apresentaremos em detalhes no próximo capítulo, possui características comuns a todos estes tipos de sistemas descritos. Como é exigido do sistema um alto grau de segurança e confiabilidade, foi necessária a introdução de técnicas automáticas de tolerância a falhas. Por outro lado, por ser operado constantemente por operadores humanos, estes poderão reconduzir o sistema ao seu estado normal, em caso de falha, além de que normalmente uma equipe de manutenção, bem treinada, pode ser acionada imediatamente após a ocorrência de uma falha.

Assim, podemos classificar o nosso sistema como sendo tolerante a falhas, reparável, que pode ser controlado manualmente e que ainda permite uma operação em modo degradado.

II.7 TÉCNICAS DE REDUNDÂNCIA (1,2,3)

As técnicas de redundância desenvolvidas para proteger os sistemas contra falhas podem ser classificadas em: técnicas de "hardware", de "software" e de "tempo".

Estas técnicas consistem na adição, ao sistema, de "hardware", "software" e execução repetida de determinadas tarefas. Para se obter um sistema tolerante a falhas eficiente é necessário aplicar estes três tipos de redundâncias convenientemente, de modo a otimizar o desempenho e o custo funcional e estrutural do sistema.

II.7.1 TÉCNICAS DE REDUNDÂNCIA DE SOFTWARE

São todos os programas, segmentos de programas, instruções e micro-instruções que são adicionados ao sistema, com o objetivo de torná-lo tolerante a falhas. Estas redundâncias são usadas para detecção e recuperação de falhas. Freqüentemente, as redundâncias de "software" são usadas em conjunto com as redundâncias de "hardware", que veremos adiante.

As três principais formas de redundância de "software" são: duplicação na memória de programa e/ou dado, rotinas de diagnóstico e todos os programas que interagem com as de redundâncias de "hardware".

Uma vantagem da redundância de "software" sobre a de "hardware", é a possibilidade de se colocar funções de tolerância a falhas depois que o projeto de "hardware" esteja pronto. Outra vantagem seria a facilidade de se fazer modificações e melhorias nas funções de tolerância a falhas depois de terem sido introduzidas no sistema.

A principal desvantagem da redundância de "software" está na impossibilidade de se garantir que os procedimentos de "software" funcionarão na presença de uma falha de "hardware", ou que eles agirão antes que os erros produzidos alterem o conteúdo dos programas e base de dados. Outras desvantagens são o alto custo de se gerar, verificar e validar os procedimentos de "software" e a dificuldade de se avaliar ou provar a eficiência destas técnicas.

II.7.2 TÉCNICAS DE REDUNDÂNCIA NO TEMPO

Estas técnicas consistem em repetir ou confirmar operações de máquina em vários níveis: micro-operações, instruções, segmentos de programas, programas, etc. Ela é normalmente empregada em conjunto com as redundâncias de "software" e "hardware".

Os dois principais objetivos da redundância no tempo são: detecção de falhas através da execução repetida de funções, e recuperação através da reinicialização de programas e repetição de operações após a detecção de um falha ou reconfiguração do sistema.

A execução repetida de um programa, com os resultados das repetições comparados ou votados majoritariamente, é certamente a forma mais antiga de detecção de falha, extremamente eficiente na detecção e recuperação das falhas transientes. Para as falhas permanentes esta técnica não é muito eficiente, pois se for produzido um erro consistente a execução repetida de um programa levará ao mesmo resultado não sendo detectada a existência da falha.

II.7.3 TÉCNICAS DE REDUNDÂNCIA DE HARDWARE

Este tipo de redundância consiste na adição de componentes de "hardware" ao sistema com a finalidade de torná-lo tolerante a falhas. Podemos subdividir esta técnica em duas partes: redundância estática e dinâmica.

II.7.3.1 REDUNDÂNCIA ESTÁTICA

Redundância estática, também conhecida como redundância por mascaramento (2,3) é introduzida no sistema de tal modo que o sinal errado, gerado pelo componente defeituoso, é mascarado (corrigido) antes que ele atinja as saídas do módulo. É importante observar que este método corrige o erro sem nenhuma mudança dinâmica na estrutura interna do sistema, por isso chama-se redundância estática. Podemos classificar este tipo de redundância pelo nível em que ela é aplicada.

II.7.3.1.1 REDUNDÂNCIA ESTÁTICA A NÍVEL DE CIRCUITO

Este é o nível mais elementar em que se pode aplicar redundância. Ela é alcançada replicando-se elementos do

circuito tais como: diodos, transistores, resistores, gates, etc., interconectando-os de tal modo a mascarar o erro causado pelo elemento defeituoso. Um exemplo é dado na figura (II.2) onde temos um diodo e um "flip-flop" quadriplicado. Com esta configuração podemos tolerar qualquer tipo de falhas simples e algumas falhas duplas e triplas.

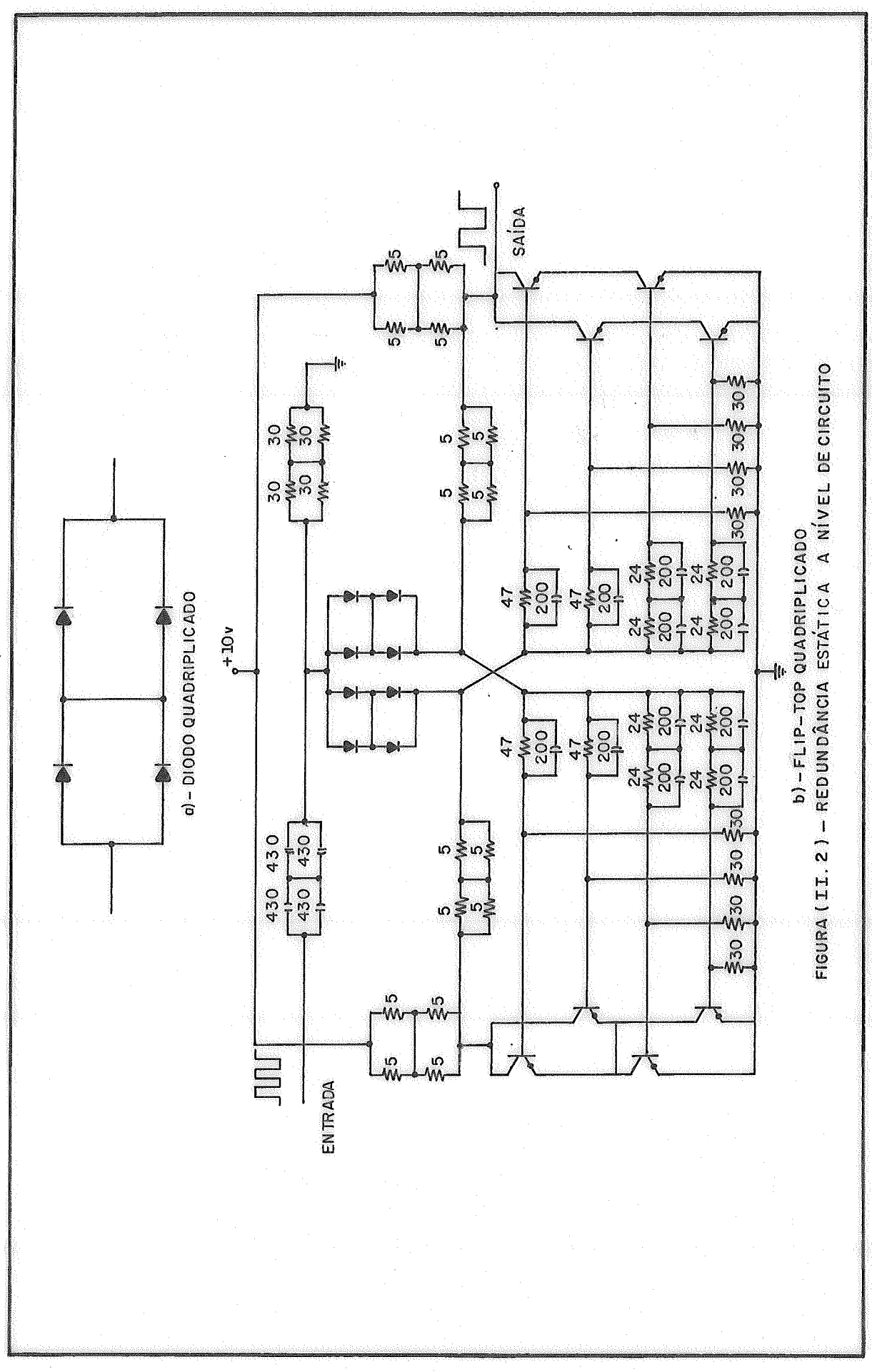
A viabilidade da redundância a nível de circuito baseia-se na hipótese da independência entre falhas de componentes. Esta técnica foi útil nas primeiras gerações de computadores, construídos com componentes discretos. Entretanto, na era dos circuitos integrados (LSI, MSI), justamente quando os custos de replicação de componentes seriam insignificantes, a redundância neste nível tornou-se menos viável devido a alta correlação entre falhas de componentes distintos dentro de um circuito integrado (1).

II.7.3.1.2 REDUNDÂNCIA ESTÁTICA A NÍVEL DE MÓDULO

Este nível de redundância baseia-se no esquema de votação majoritária proposto por J. Von Newmann em 1956 (1) , como está ilustrado na figura (II.3). Quando o módulo for triplicado como na figura, chama-se esta técnica de redundância tripla modular (em Inglês TMR).

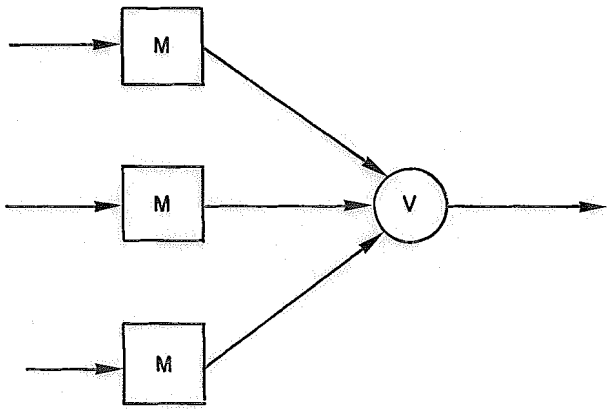
O módulo replicado deve ser grande o suficiente para constituir unidade fisicamente separada, possibilitando que possua integrados, embalagem, alimentação, etc., próprios, preservando a independência entre falhas nos módulos, que é essencial para aplicação desta técnica.

A redundância estática a nível de módulo parece ser compatível com o estado atual da tecnologia de fabricação de LSI. Como o custo dos componentes está cada vez mais baixo, este tipo de redundância está se tornando mais viável.

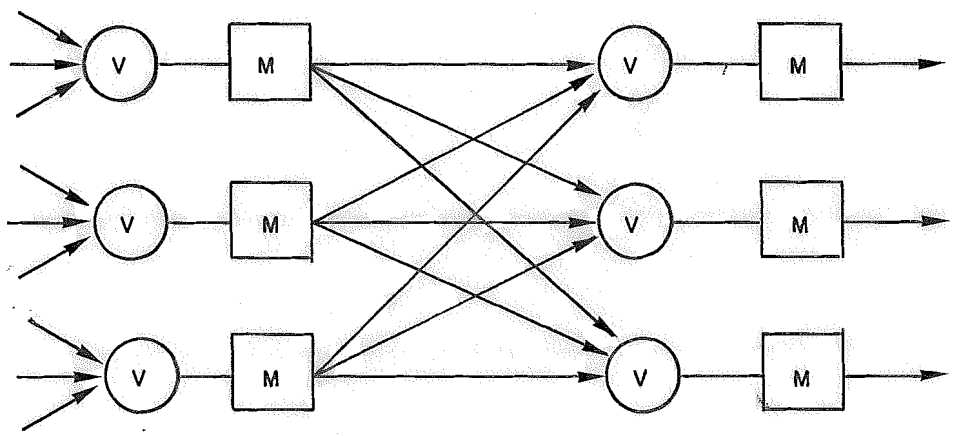


b) - FLIP-TOP QUADRIPLICADO

FIGURA (II. 2) - REDUNDÂNCIA ESTÁTICA A NÍVEL DE CIRCUITO



a – VOTADORES NÃO REPLICADOS



b – COM VOTADORES REPLICADOS

FIGURA (II.3) – ESQUEMA DE VON NEWMANN

II.7.3.1.3 VANTAGENS E DESVANTAGENS DA REDUNDÂNCIA ESTÁTICA

Como vantagens da redundância estática podemos citar a capacidade de mascarar falhas instantaneamente, permitindo a execução contínua dos programas. Outra vantagem seria um menor custo de "software", já que este seria bem mais simples, bastando uma eventual sincronização entre os módulos.

As principais desvantagens são: aumento no custo, volume, consumo da fonte de alimentação, etc., tudo devido a replicação do "hardware". Também para a redundância a nível de circuito podemos citar a dificuldade na localização do componente defeituoso.

II.7.3.2 REDUNDÂNCIA DINÂMICA

A aplicação da redundância dinâmica consiste na eliminação das falhas causadoras de erros que aparecem nas saídas dos módulos. A tolerância a falhas é implantada em três etapas: primeiro é feita a detecção da falha, depois a localização e por último são tomadas medidas para restauração do sistema, eliminando-se as falhas ou corrigindo-se os erros.

Os sistemas redundantes dinamicamente empregam o uso combinado de técnicas de redundância de "hardware", "software" e tempo. O uso deste tipo de sistema exige um grande número de decisões na fase de projeto tais como: nível de modularização, técnicas de detecção de falhas, tipos de ações para restauração, proteção, comunicação entre módulos, etc.

II.7.3.2.1 DETECÇÃO DE FALHA

A detecção de uma falha em um sistema redundante dinamicamente geralmente é implementada fazendo-se uma verificação de erros. Freqüentemente, permite-se que os erros produzidos por uma falha propaguem-se até as saídas do módulo para permitir que os mecanismos de verificação detectem a existência desta falha.

Normalmente, dentro de uma CPU ou memória, onde há uma grande movimentação e transformação de dados, deseja-se que a detecção de um erro seja feita o mais breve possível, permitindo que o sistema reaja, impedindo a propagação do erro, tornando mais fácil a recuperação . Para se conseguir esta capacidade de detecção pode-se usar mecanismos de "hardware" tais como código de paridade, proteção de áreas de memória, códigos de detecção de erros nas comunicações, etc.

Por outro lado, estes mecanismos de detecção também podem ser implantados por "software", conseguindo assim mecanismos de alta flexibilidade e baixo custo. Podemos citar como exemplos: verificação das interfaces de I/O do módulo, "checksumming" para detectar erros em arquivos, rotinas de auto-diagnóstico executadas periodicamente,etc.

De um modo mais geral, visualizamos dois níveis de detecção (observação) da ocorrência de uma falha: mecanismos internos ao módulo, que são mecanismos incorporados ao módulo e mecanismos externos de observação do módulo, que analisam as saídas produzidas tentando detectar a existência de uma falha.

II.7.3.2.2 LOCALIZAÇÃO DA FALHA

Depois de detectada a existência de uma falha, em um sistema com redundância dinâmica, é preciso localizá-la para saber quais serão as medidas que devem ser tomadas para reconduzir o sistema ao seu estado normal de operação. O problema da localização da falha também é conhecido por diagnóstico da falha.

Embora a detecção de uma falha normalmente já traga em si algumas informações de diagnóstico, alguns sistemas precisam de informações extras sobre a fonte de erros. Nestes casos é comum a existência de programas especiais para diagnósticos de erros. Para sistemas fechados é suficiente a localização a nível de módulo e conseqüentemente a substituição automática deste

módulo. Para os sistemas onde é permitida a manutenção manual, pode-se executar rotinas que auxiliem a equipe de manutenção na sua tarefa.

II.7.3.2.3 RECUPERAÇÃO

Após uma falha ter sido detectada e localizada, o sistema deve iniciar procedimentos para isolar esta falha, eliminando futuros distúrbios que ela pudesse vir a provocar.

Em alguns sistemas, chamados autoreparáveis, os módulos defeituosos são isolados e os sobressalentes são chaveados para assumir as funções daqueles. Estes módulos agem de um modo passivo, pois enquanto eles não estão em operação não participam do processamento.

Em outros sistemas, chamados parcialmente tolerantes a falhas ou suavemente degradáveis, após se detectar, localizar e isolar uma falha o sistema continua o seu processamento em um modo degradado.

Em qualquer caso, após o sistema ter conseguido uma configuração livre de falhas alguns procedimentos são necessários, tais como: recarregamento dos programas perdidos que são feitos a partir de arquivos armazenados em memória não volátil, restauração da base de dados, reescalamento de tarefas interrompidas, etc.

Um número considerável de sistemas admitem a manutenção manual das partes defeituosas. Nestes casos a equipe de manutenção deve ser rapidamente acionada antes da ocorrência de uma segunda falha, quando então haveria muito maiores dificuldades de reparo.

II.7.3.3 REDUNDÂNCIA HÍBRIDA

Como o nome indica, a redundância híbrida consiste no uso em conjunto de redundâncias estáticas e dinâmicas para se conseguir a tolerância a falhas.

Um sistema típico é mostrado na figura (II.4), onde além das redundâncias estáticas (a nível de módulo) temos unidades sobressalentes para substituir aquelas defeituosas. A votação majoritária garante a correção da saída além de proporcionar a detecção e localização da falha, parâmetros muito importantes no sucesso do uso de redundância dinâmica. A possibilidade de se chavear os módulos sobressalentes no lugar dos defeituosos, garante o esquema de votação completo até que se esgote o estoque de módulos sobressalentes. O fato de se ter várias cópias dos módulos ativos permite a implementação de um mecanismo fácil de recuperar os programas e dados perdidos, possibilitando também a fácil re-sincronização do sistema.

A principal dificuldade técnica na elaboração deste esquema está na implementação dos mecanismos de chaveamento, o que dependendo da complexidade do "hardware", pode inviabilizar o sistema. Este problema tem sido assunto de profundas pesquisas nos últimos anos.

II.8 METODOLOGIA PARA PROJETOS DE SISTEMAS TOLERANTES A FALHAS

Os projetistas de sistemas tolerantes a falhas ao introduzir em seus sistemas técnicas de proteção contra falhas seguem um procedimento sistemático de quatro passos (2,3).

i - Os requisitos computacionais devem ser estudados e a arquitetura do sistema é especificada supondo-se inicialmente que o sistema esteja imune a falhas;

ii - É feita uma caracterização e uma classificação das falhas que devem ser toleradas;

iii - Projeta-se técnicas de detecção, localização e recuperação, para proteger o sistema das falhas identificadas no item ii, modificando-se a arquitetura do sistema para incorporar as técnicas propostas;

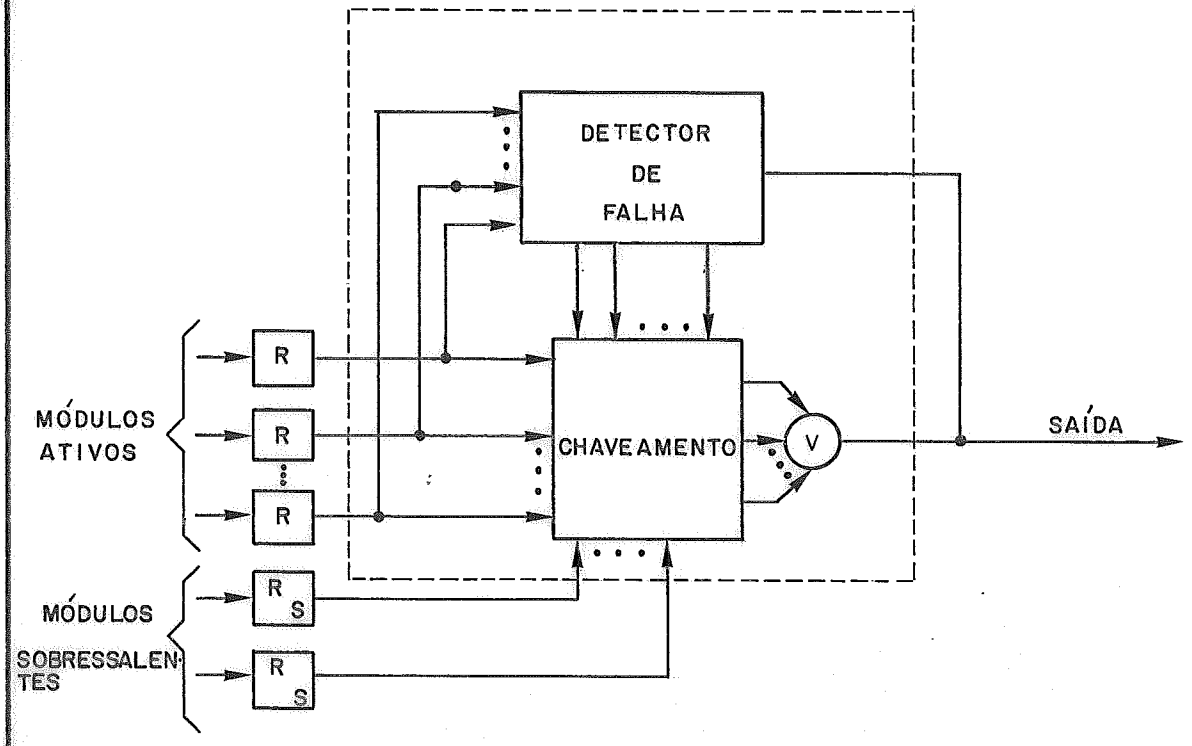


FIGURA (II.4) — REDUNDÂNCIA HÍBRIDA

iv - Faz-se a estimativa analítica ou experimental da eficiência das técnicas de tolerância a falhas propostas no item iii.

A experiência mostra que geralmente os resultados obtidos no ítem iv levam o projetista a aperfeiçoar o ítem iii num processo iterativo até que se consiga uma solução adequada.

Os próximos capítulos descrevem o trabalho que realizamos adotando esta metodologia.

CAPITULO III

PROJETO DE UM CENTRO DE SUPERVISÃO PARA SISTEMAS ELÉTRICOS.

III.1 INTRODUÇÃO

Um centro de supervisão e controle, como o próprio nome indica, tem como funções básicas supervisionar e controlar algum tipo de processo. Estes sistemas são conhecidos na literatura internacional pela sigla "SCADA" (Supervisory Control And Data Aquisition). Podemos citar como áreas de aplicação destes sistemas alguns setores como (7):

- Geração, transmissão e distribuição de energia elétrica;
- Transporte e distribuição de gases e líquidos;
- Distribuição de água potável ou industrial;
- Distribuição e transferência de calor;
- Controle de tráfego (rodoviário, ferroviário e aéreo);
- Transmissão de dados;
- Supervisão e controle de complexos de edifícios e plantas industriais.

A equipe de eletrônica digital do CEPEL vem desenvolvendo projetos na área de supervisão e controle, que atendam às necessidades das empresas brasileiras no setor de energia elétrica. Embora o projeto que será descrito neste trabalho possa ser usado no controle de outros processos, aqui toda atenção estará fixada em aplicações que envolvam o setor elétrico.

III.2 DESCRIÇÃO DAS FUNÇÕES DE UM CENTRO DE SUPERVISÃO PARA SISTEMAS ELÉTRICOS

O controle de sistemas elétricos é hierarquizado (8). No topo da hierarquia está a central de controle, seguida pelos centros de controle das companhias, regionais e locais. No

nível mais baixo estão os processos que serão controlados, no caso as subestações e usinas. A figura (III.1) apresenta um sistema típico para supervisão e controle na área de energia elétrica (7).

Cada centro tem como função coletar e processar dados relevantes à operação do sistema elétrico, transformar esta massa de dados para uma forma legível ao operador humano, realizar controles e tomar decisões apropriadas.

Concluindo, um sistema de supervisão e controle para energia elétrica é um complexo homem-máquina, envolvendo vários computadores, localizados em locais geograficamente distantes, executando simultaneamente múltiplas funções.

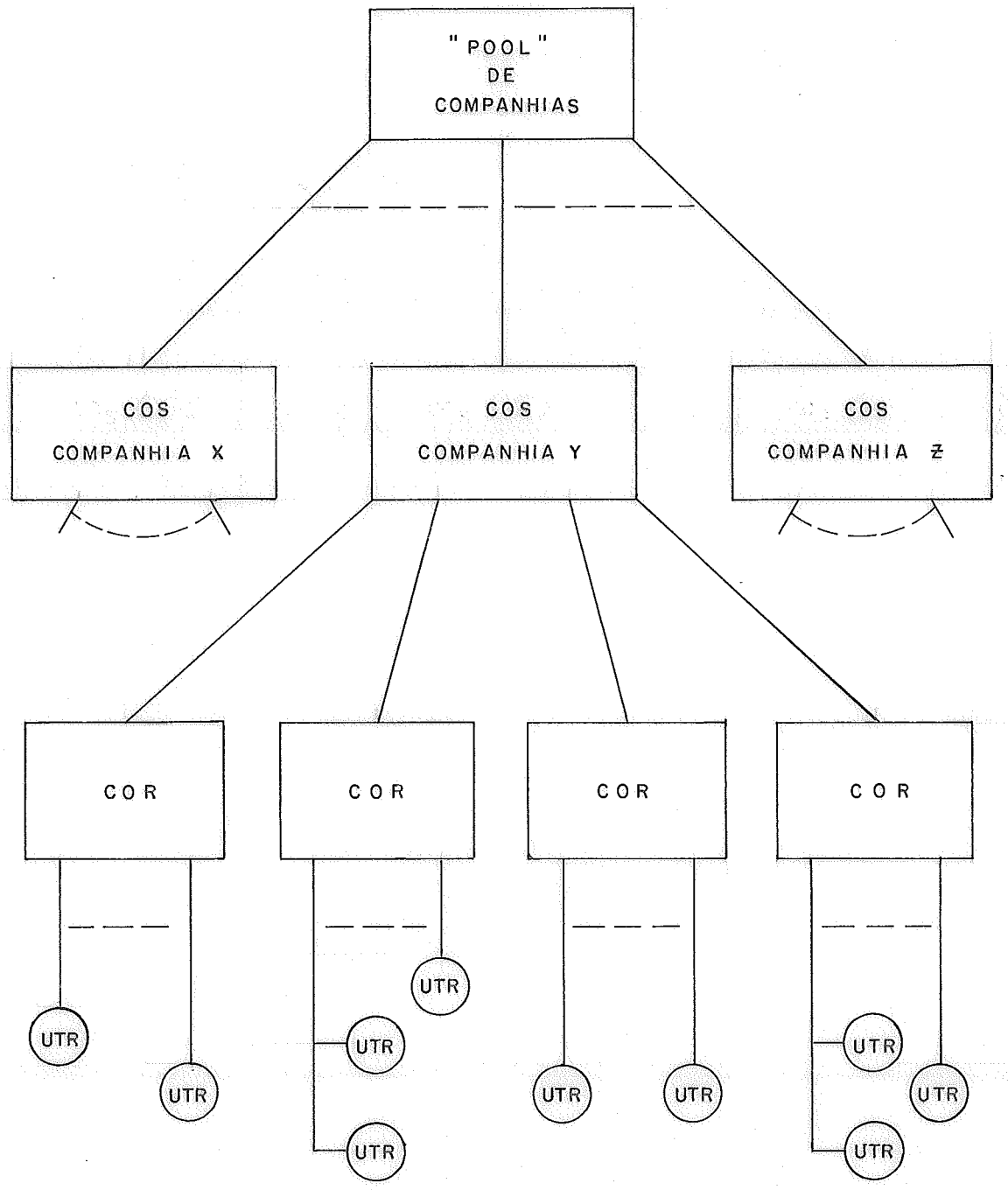
Na estrutura apresentada na figura (III.1) o CEPEL primeiro desenvolveu uma unidade de terminal remoto (6), subindo um pouco mais na hierarquia desenvolveu em cooperação com FURNAS Centrais Elétricas S.A. o projeto de um centro de supervisão para equipar despachos regionais (COR).

Os despachos regionais têm como principal função: coordenar as manobras, controlar o valor de tensão e normalizar o sistema elétrico após perturbações, agindo dentro de uma área prédeterminada do sistema elétrico (9).

Dentro de um despacho regional são executadas as seguintes atividades (9):

i - PRÉ-DESPACHO

- Estudo das anormalidades e previsões de normalização de equipamentos;
- Análise e coordenação do desligamento de equipamentos;
- Definição das sequências de operações normais para a rede.



C.O.S – CENTRO DE OPERAÇÃO DO SISTEMA.

C.O.R – CENTRO DE OPERAÇÃO REGIONAL

U.T.R – UNIDADE DE TERMINAL REMOTO

FIGURA (III.1) SISTEMA DE SUPERVISÃO PARA ENERGIA ELÉTRICA.

ii - DESPACHO

- Controle de tensão das barras;
- Normalização do sistema elétrico após perturbações;
- Emissão de ordens de manobras: isolamento de equipamento, isolamento de proteção, etc.;
- Coordenação da execução de testes em equipamentos de teleproteção;
- Coordenação da execução de testes de energização de novos equipamentos;
- Aprovação da execução de serviços em usinas e subestações, que não necessitem de desligamento;
- Coordenação da execução de trabalhos em linha-viva;
- Supervisão dos equipamentos da sala de controle;
- Registro de leituras de medidas e posição de derivação dos transformadores.

iii - PÓS-DESPACHO

- Levantamento dos dados referentes a perturbações;
- Registro de leituras das medidas de faturamento;
- Elaboração de relatórios diários com principais ocorrências no sistema;
- Registro de valores de fluxo de potência, sob solicitação.

Devido à grande quantidade de dados manipulados nestes centros, o valor elevado de energia a ser controlada, as grandes distâncias envolvidas e às sérias conseqüências que uma pane, ou operação indevida da rede elétrica podem causar, justifica-se o alto índice de disponibilidade e segurança exigidos dos equipamentos usados no COR, obrigando a introdução no projeto dos mesmos de técnicas que possibilitem sua tolerância a falhas.

A figura (III.2) apresenta o esquema funcional de um centro de supervisão regional típico (10).

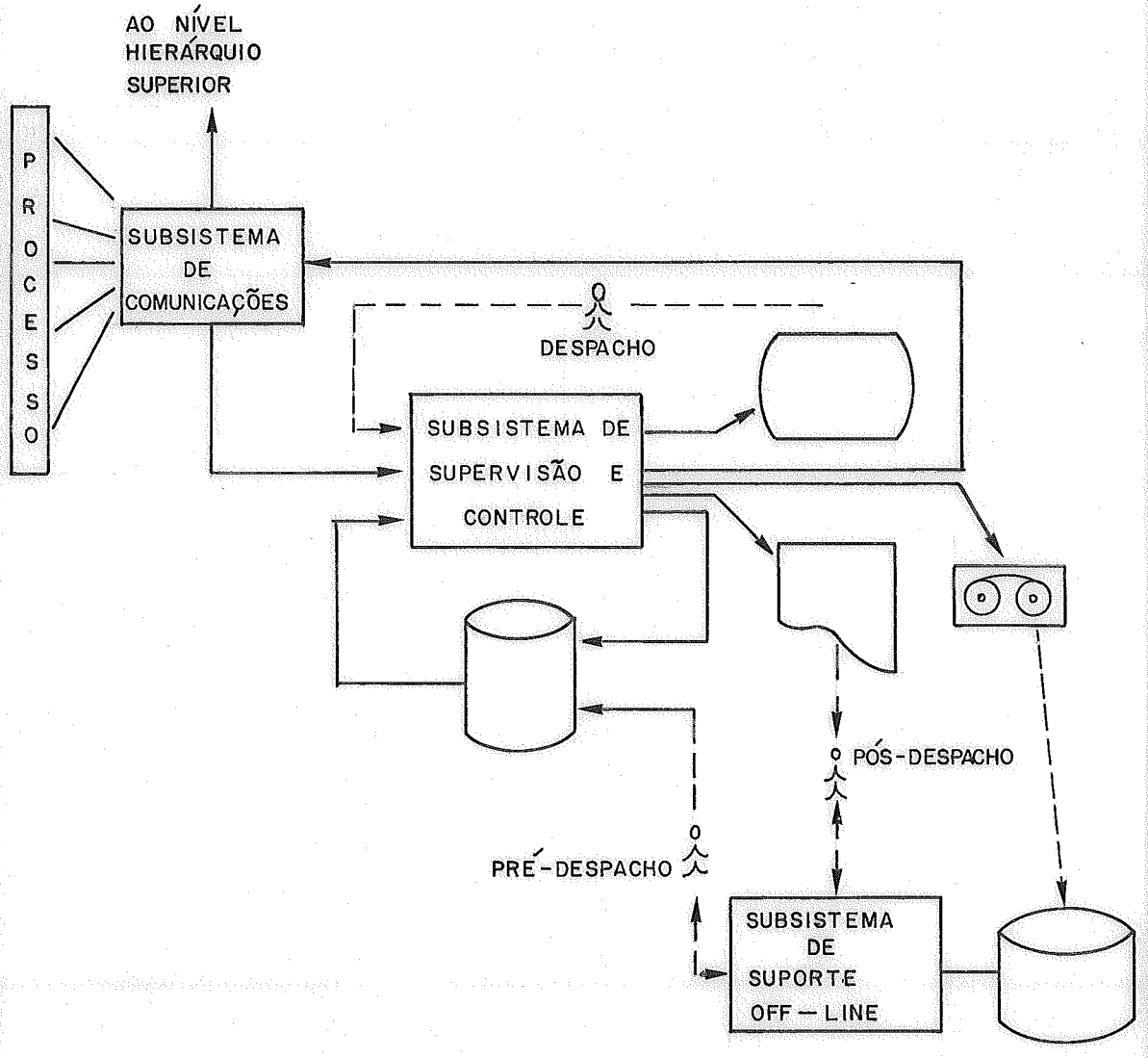


FIGURA III.2 — ESQUEMA GERAL DE UM CENTRO DE SUPERVISÃO — MODELO CLÁSSICO

Por este modelo pode-se dividir um centro de supervisão nos seguintes subsistemas:

i - Subsistema de Comunicações ("Front-End"): É o responsável pelas comunicações com o mundo externo. Realizando troca de mensagens com o processo controlado, permitindo o fluxo de dados para centros em níveis hierárquicos superiores ou em plano paralelo;

ii - Subsistema de Supervisão e Controle "On-Line": É o responsável pela execução das rotinas durante a operação de despacho, em interação permanente com o homem e pelo fornecimento de dados para análise posterior;

iii - Subsistema de Suporte "Off-Line": Serve às atividades de análise de pós-despacho e de pré-despacho. Suporta ainda atividades de manutenção e alteração de programas e arquivos.

Tradicionalmente, as funções de um centro de supervisão têm sido implantadas em um sistema de mini-computadores em redundância dupla. A figura (III.3) apresenta um exemplo de uma configuração típica para um centro de supervisão clássico.

Entretanto, o avanço tecnológico na produção de circuitos integrados (LSI) e a redução dos custos de fabricação dos microprocessadores, viabilizaram a utilização destes dispositivos, para a constituição de centros de supervisão.

Algumas vantagens que os sistemas com processamento distribuído apresentam sobre os centralizados são (11):

i - Modularidade: É uma característica inerente quando se distribui a inteligência utilizando microprocessadores. Por usarem elementos mais simples, tanto de "hardware" quanto de "software", permitem a divisão do sistema em pequenos módulos, mais simples de serem implementados

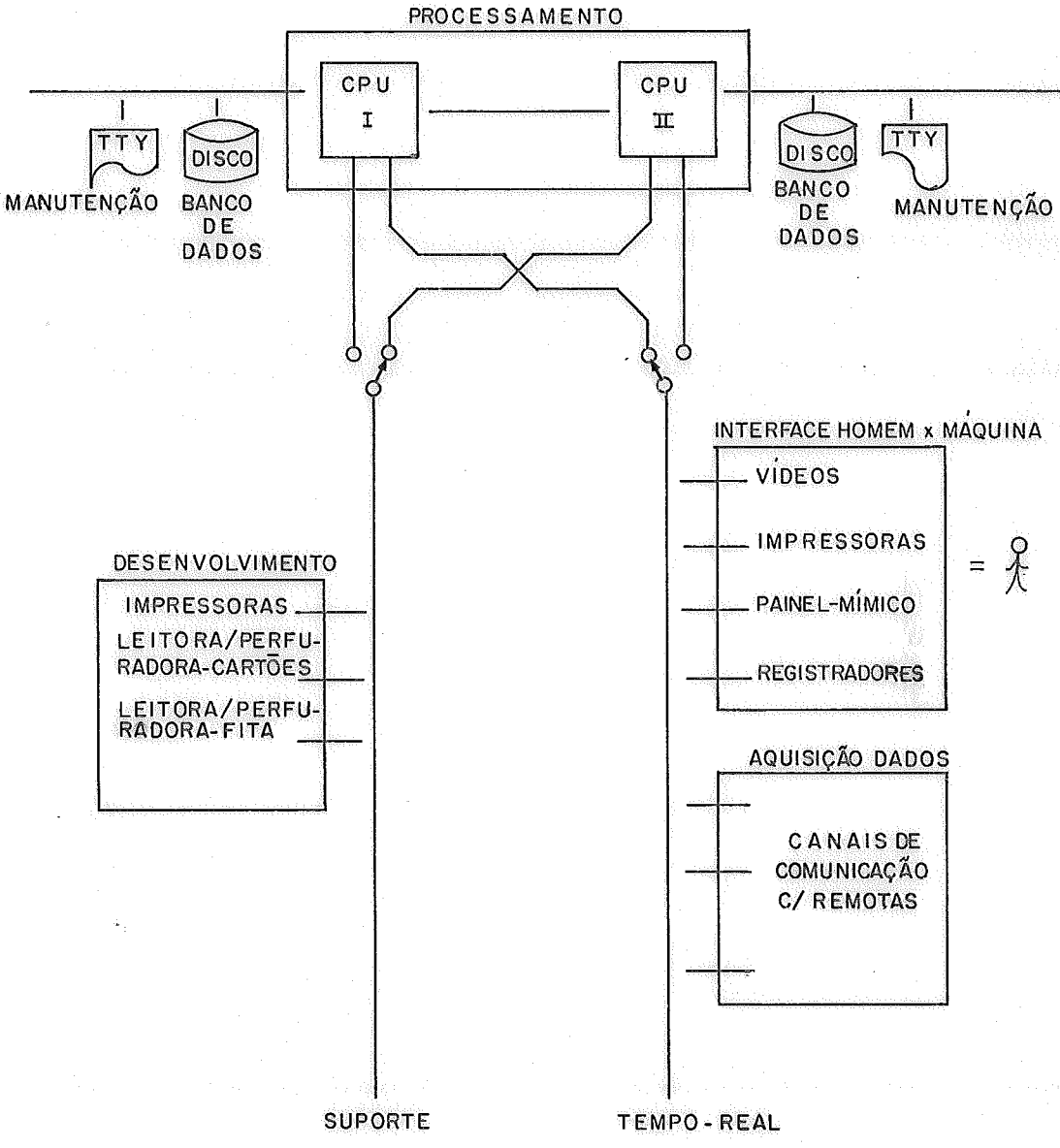


FIGURA (III.3) SISTEMA CLÁSSICO

FONTE: WESTINGHOUSE

testados, reparados,etc.

ii - Capacidade de expansão: Esta característica é decorrente da primeira, permitindo que o usuário comece com pequenas configurações, sem ter que pagar por mais do que o necessário. Por outro lado, sempre que o usuário desejar expandir seu sistema, basta comprar os módulos necessários para isto;

iii - Alto índice de disponibilidade: Justifica-se esta vantagem pelas seguintes características dos sistemas distribuídos:

a - Usando elementos mais simples, tanto de "software" quanto "hardware", o sistema fica menos vulnerável a falhas;

b - Possuindo a inteligência distribuída o sistema pode trabalhar em modo degradado, e a independência entre os módulos evita a contaminação devido a uma falha em um determinado módulo;

c - A redundância do sistema pode ser planejada de modo a utilizar Y módulos sobressalentes para X módulos ativos (Y menor que X), isto é, consegue-se um alto índice de disponibilidade sem haver duplicação do sistema inteiro (12), como ocorre em sistemas centralizados.

Estes fatos tornaram questionáveis as estruturas tradicionais dos centros de supervisão, principalmente aqueles onde se exige pouca capacidade de processamento matemático.

A figura (III.4) apresenta um modelo moderno de um centro de supervisão. Neste modelo atribui-se inteligência a todos os periféricos, colocando-se um microprocessador dedicado ao controle de cada um deles. Qualquer módulo pode se comunicar com qualquer outro através da rede de interconexão. A seguir

será feita uma descrição detalhada desta arquitetura utilizada em nosso projeto.

III.3 DESENVOLVIMENTO DO PROJETO

III.3.1 INTRODUÇÃO

Ao se projetar o centro de supervisão procurou-se obter uma estrutura simples, de fácil comercialização para a indústria nacional, cujo mercado não ficasse restrito apenas ao setor elétrico, podendo cobrir um vasto mercado de controle de processos industriais com as seguintes especificações (10):

i - Geograficamente extensos (supervisão de redes de energia, transporte, hidrométricas, etc.) ou medianamente extensos (supervisão de refinarias, destilarias, fábricas de cimento, celulose, etc.);

ii - De operação em malha aberta, isto é, com as decisões a cargo do homem;

iii - Com requisitos de processamento matemático relativamente modestos;

iv - De tempos de resposta relativamente lentos (segundos);

v - Especificados para uma longa vida útil (dez anos);

vi - De alta taxa de crescimento horizontal (crescimento médio das instalações em torno de 5% ao ano);

vii - Com sérias dificuldades de manutenção de periféricos importados, podendo acompanhar a evolução dos periféricos nacionais (transportadores, modems, impressoras, terminais de vídeo, etc.).

O projeto está basicamente dividido em duas partes: sistema básico e sistema de aplicação. A figura (III.5) apresenta um quadro com a subdivisão destes sistemas.

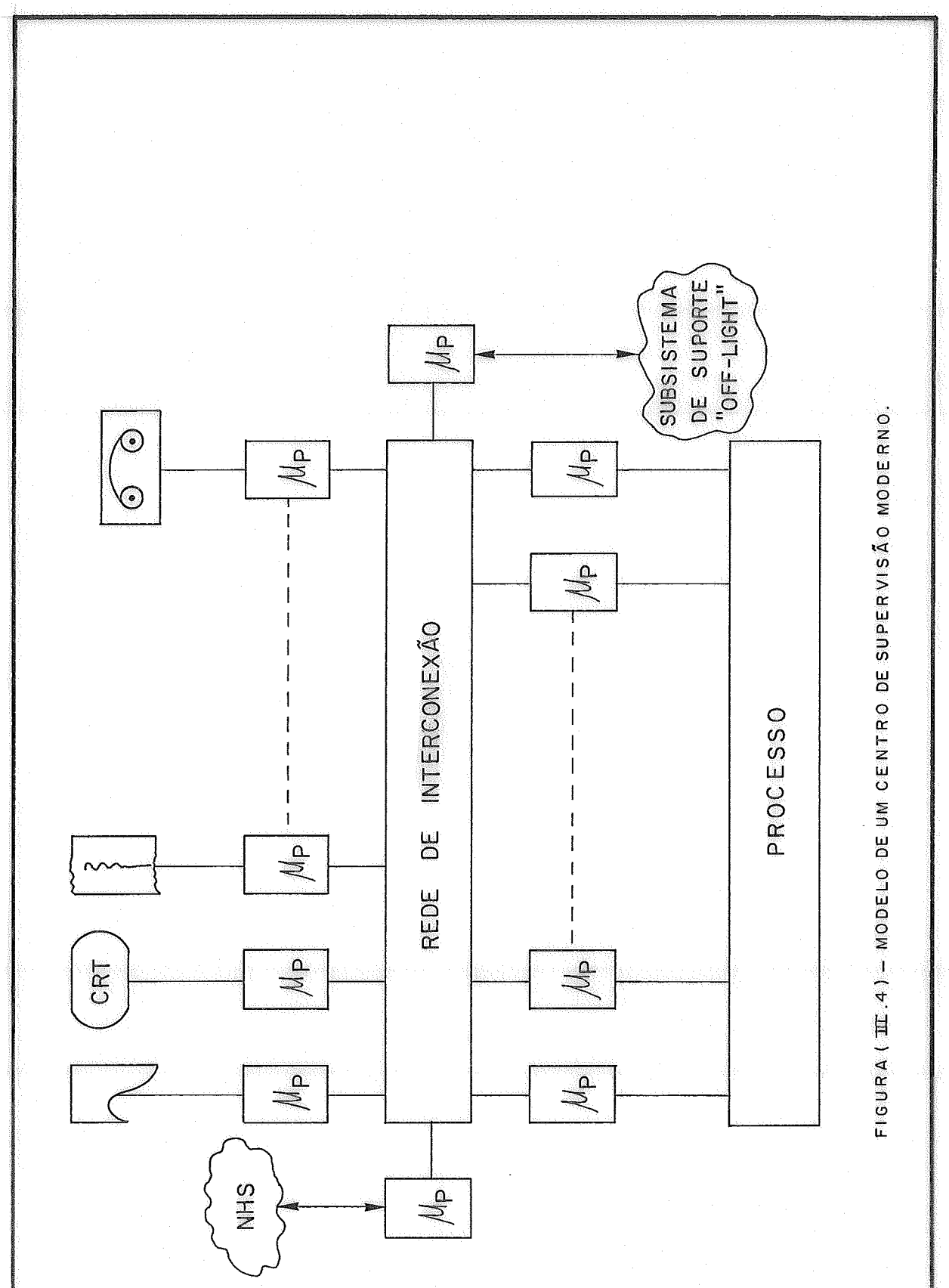
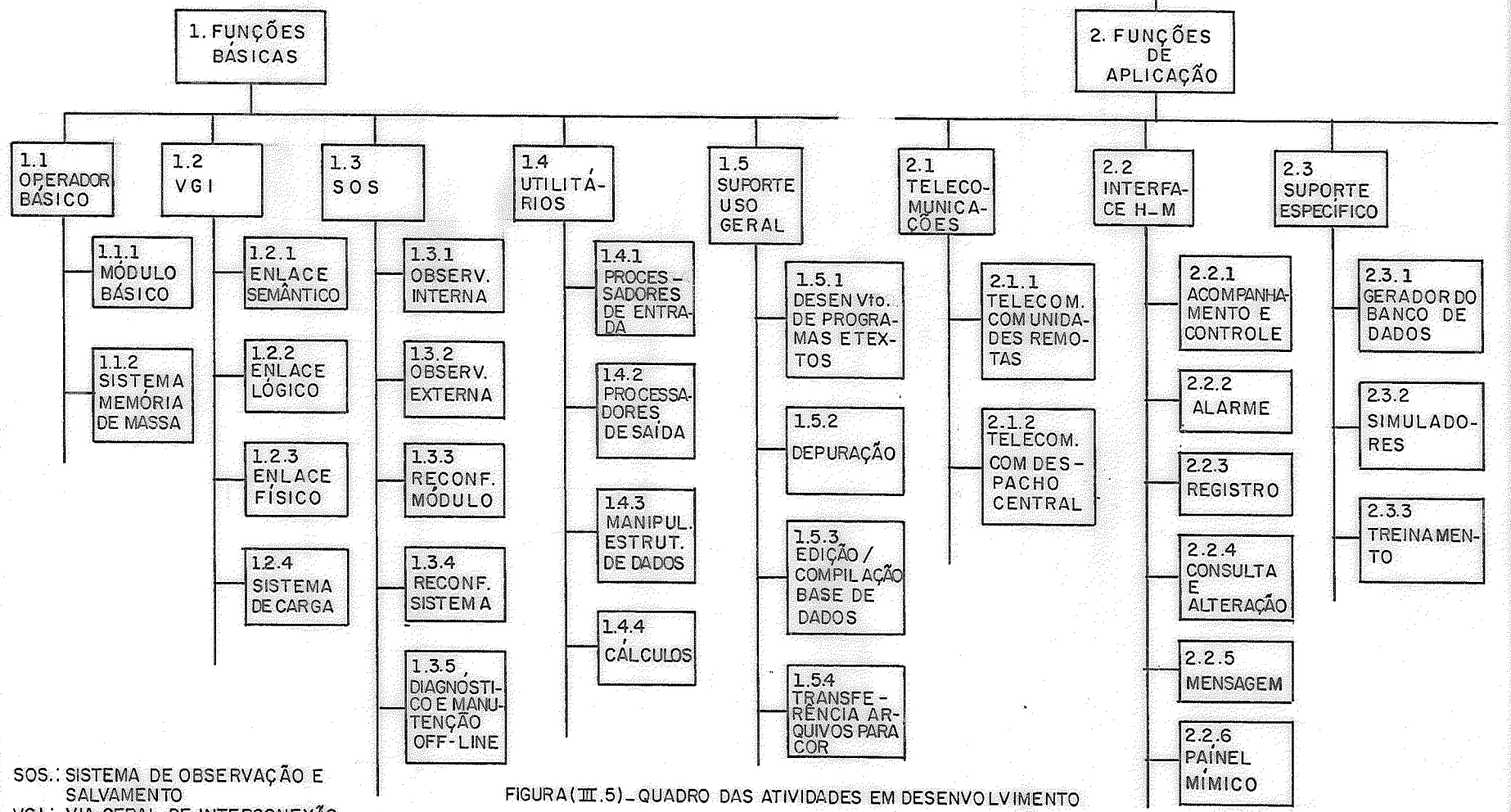


FIGURA (III.4) – MODELO DE UM CENTRO DE SUPERVISÃO MODERNO.



SOS.: SISTEMA DE OBSERVAÇÃO E SALVAMENTO
VGI.: VIA GERAL DE INTERCONEXÃO

FIGURA (III.5) - QUADRO DAS ATIVIDADES EM DESENVOLVIMENTO

III.3.2 SISTEMA BÁSICO

O sistema básico consiste na parte do projeto independente da aplicação, podendo ser utilizado por outras empresas e produzido em escala industrial.

As partes que compõem o sistema básico são:

i - Módulo básico;
ii - Sistema de comunicação intermódulos.
iii- Sistema de observação e salvamento (SOS);
iv - Utilitários;
v - Suporte "off-line" de uso geral.

A figura (III.6) apresenta de um modo simplificado a estrutura do centro de supervisão proposto. Neste, cada operador recebe uma função específica dentro do sistema. A ele são incorporados todos os dispositivos necessários à realização das tarefas que lhe foram atribuídas. O funcionamento de cada operador é completamente independente dos outros. O único vínculo entre os módulos é a rede de interconexão (VGI), que é o mecanismo responsável pela comunicação entre os módulos.

III.3.2.1 MÓDULO BÁSICO

O módulo básico é composto de uma parte fixa, que se repete para todos os operadores do sistema e de uma parte que muda em função do periférico acoplado ao operador.

O módulo básico é composto das seguintes partes:

i - Uma unidade de processamento central (13) baseada em um microprocessador de 16 bits (o uso de um microprocessador sofisticado justifica-se para tornar o equipamento competitivo em termos de tecnologia internacional);

ii - Memória de até 128 Kbytes (13) formado por uma combinação

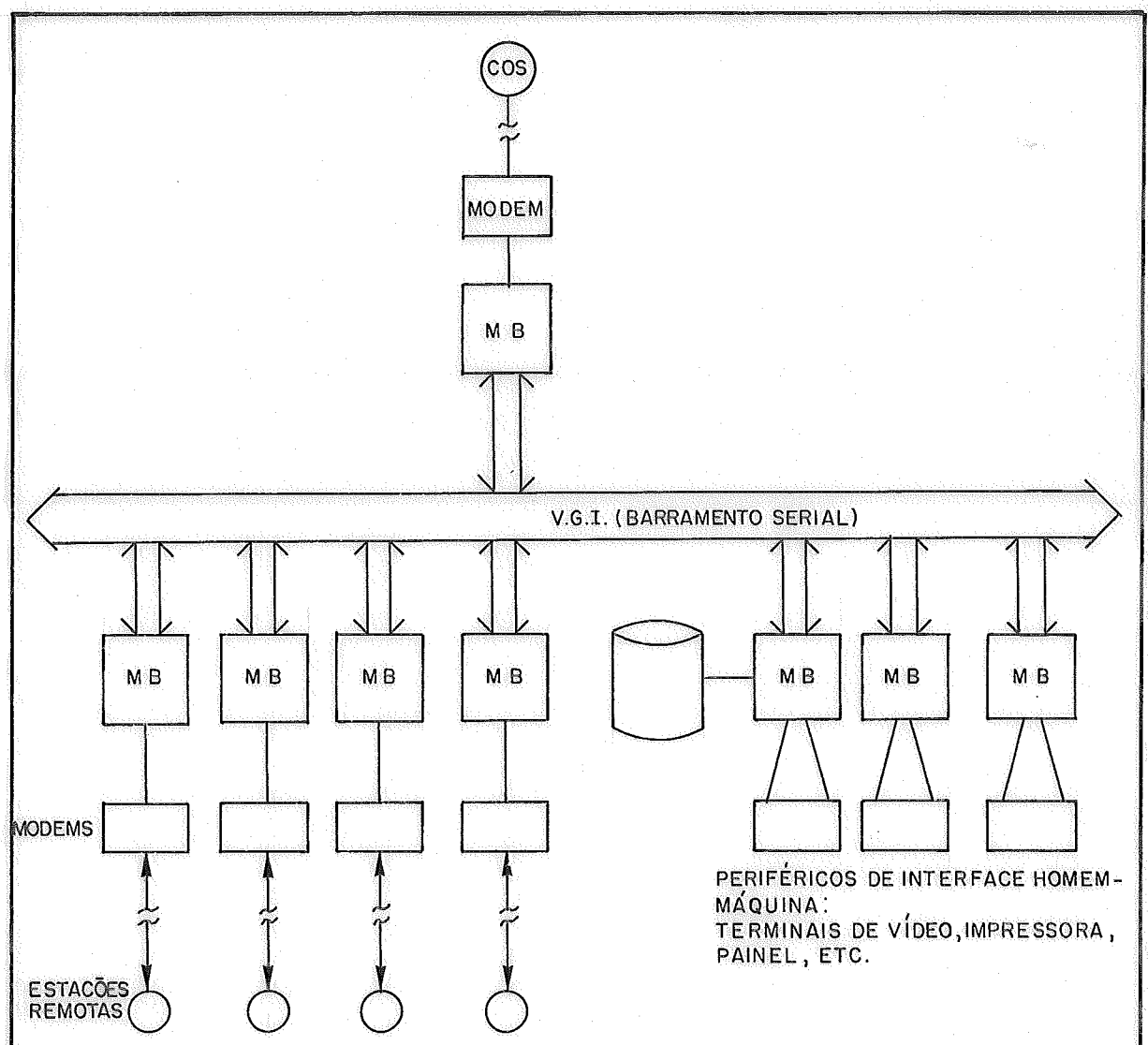


FIGURA (III.6) - ESTRUTURA SIMPLIFICADA DO CENTRO DE SUPERVISÃO

de integrados do tipo EPROM e/ou RAM. (Neste ponto se concentra o grande volume em termo de componentes de "hardware" importados);

iii - Interfaces para periféricos de entrada e saída (13). Podemos citar uma grande variedade de periféricos usados: modens, impressoras, terminais coloridos, memória de massa (disco tipo Winchester), registradores gráficos, etc.;

iv - Circuitos para acoplamento do operador com a rede interna de comunicação (13): que consiste num conjunto de dispositivos para estabelecer o protocolo físico de uma rede do tipo ETHERNET;

v - Sistema operacional em tempo real (11,14). Possui a capacidade de gerenciar múltiplas tarefas. As tarefas são codificadas separadamente em função de cada evento que se deseja controlar. Um número variável de tarefas podem ser executadas concorrentemente e comunicar-se por meio de mensagens, compartilhando recursos comuns.

Para atender os eventos que ocorrem periodicamente, o sistema suporta um relógio que fornece ao módulo a temporização necessária para despertar as tarefas cuja função esteja relacionada com o tempo. O sistema operacional possui ainda mecanismos para o tratamento de interrupções, que são codificados como mensagens especiais geradas por eventos externos.

A cada tarefa é atribuída uma prioridade, que está relacionada com o grau de importância da tarefa dentro do sistema. A partir desta prioridade o escalador escolhe dentre aquelas que disputam o acesso à CPU qual será executada em um dado instante.

O núcleo do sistema operacional foi quase totalmente (98%) escrito em linguagem de alto nível (PL/M), o tamanho da área de código do núcleo é de cerca de 1500

bytes e da área de variáveis de cerca de 180 bytes. Uma operação de envio de mensagem (SEND) utiliza no máximo 350us de tempo de processamento e uma operação de espera (WAIT) no mínimo 270us.

III.3.2.2 SISTEMA DE COMUNICAÇÃO INTERMÓDULOS (VIA GERAL DE INTERCONEXÃO - VGI) (15)

III.3.2.2.1 INTRODUÇÃO

A comunicação entre módulos é realizada através da troca de mensagens. Cada operador possui duas partes: a parte mestre, que toma a iniciativa da comunicação e a parte escrava, que responde a esta iniciativa.

O protocolo empregado usa uma filosofia de acesso à via do tipo ETHERNET ("CARRIER SENSE MULTIPLE ACCESS WITH COLLISION DETECCION - CSMA/CD") (16,17), usando uma codificação derivada da codificação Manchester, sendo o protocolo físico estruturado segundo as normas do SDLC.

O uso de um meio passivo (fio) e a ausência de qualquer elemento ativo permitem a obtenção de um sistema altamente confiável (pois ele é pouco sensível aos efeitos de uma falha), além de facilitar a manutenção (módulos defeituosos podem ser desconectados sem que a rede saia de serviço), permitindo ainda o uso de comunicação em "broadcasting".

III.3.2.2.2 ESTRUTURA DA VGI

Devido à complexidade de uma rede quando vista como um todo, costuma-se organizá-las de uma forma hierarquizada, em níveis (camadas). Assim, sobre o nível mais elementar, que é constituído pelas ligações físicas entre os operadores, assentam-se sucessivamente novos níveis que se utilizam dos serviços oferecidos pelos níveis inferiores para realizar novas funções que são oferecidas aos níveis superiores.

Com esta metodologia fica transparente para os usuários (programas de aplicação) os diversos procedimentos para execução das intercomunicações. Desta forma, estes não precisam se preocupar com a topologia da rede, os métodos de acesso à via, ao meio utilizado para transmissão ou mesmo o "hardware" empregado.

A figura (III.7) apresenta de um modo esquemático a estrutura em níveis adotada para implementação da VGI. Estes níveis foram estruturados para se conseguir dois objetivos básicos (18):

i - Cada nível deverá ser operacionalmente auto-suficiente para que mudanças nele não acarretem mudanças consideráveis nos outros níveis;

ii - Os procedimentos nos níveis mais internos deverão ser transparentes aos níveis mais externos.

1 - NÍVEL DO HARDWARE (H)

Realiza a transferência de uma informação ("bytes", palavras,etc.) utilizando-se de sinais elétricos. Isto envolve a definição do meio de transmissão, voltagem, tempo de duração de "bits", circuitos e dispositivos microperiféricos, técnicas de transmissão como: serial, síncrono ou assíncrono, half-duplex, full-duplex, etc.

2 -NÍVEL DO ENLACE FÍSICO (HV)

Realiza a transferência de uma mensagem utilizando-se da troca de informações (funcionais e operacionais) como unidade de trabalho. É composto pelas rotinas "software" básico ("Handlers" da VGI) que controlam diretamente os dispositivos de "hardware". Este nível se preocupa com a formatação da mensagem, inserção e decodificação de códigos para verificação de erros, etc.

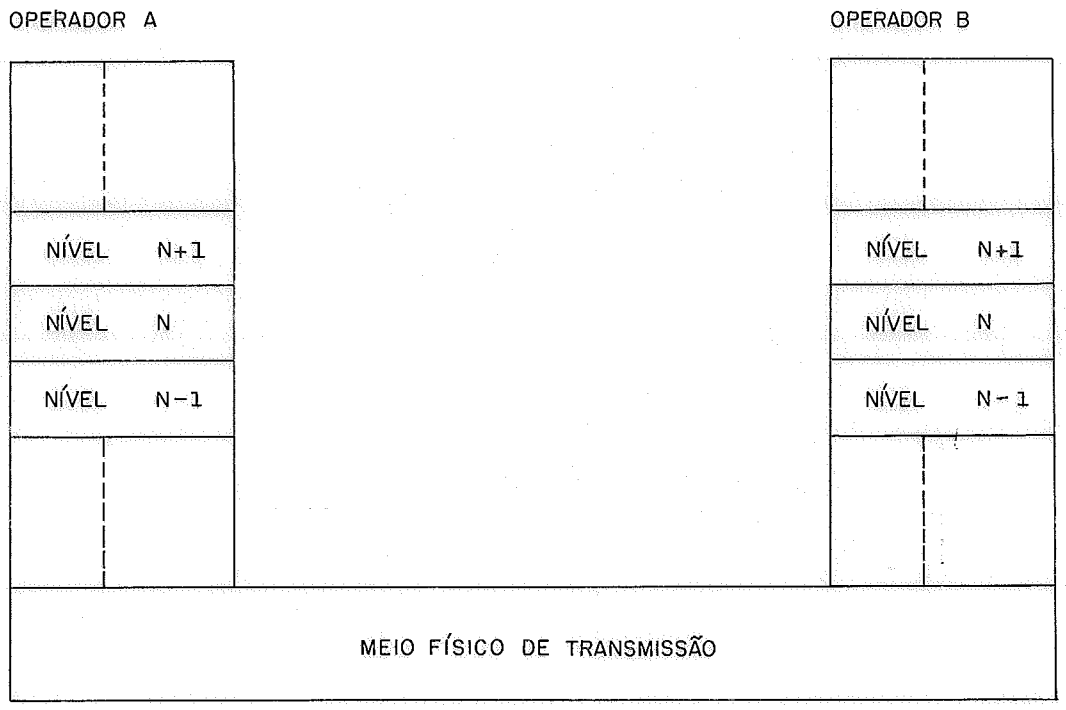


FIGURA (III.7) – ESTRUTURA EM NÍVEIS DA VGI

3 - NÍVEL DO ENLACE LÓGICO (PV)

Realiza uma unidade de comunicação (diálogo) utilizando troca de mensagens como unidade de trabalho. Contém os programas dedicados à VGI. Devido à assimetria do diálogo, o enlace lógico apresenta duas partes: uma para o mestre, outra para o escravo. Este nível se preocupa com a lógica das operações tipo pergunta-resposta, assegurando o fluxo das mesmas, detectando "time-outs", "dead-locks",etc.

4 - NÍVEL DO ENLACE SEMÂNTICO (SV):

Permite ao usuário (processos de aplicação) a realização de um conjunto de funções, de alto nível, para a transmissão e recepção de mensagens. Este nível procura fornecer serviços, de modo a mascarar detalhes de processamentos trabalhosos, repetitivos ou que não estejam ligados diretamente com os objetivos da aplicação.

5 - NÍVEL DO USUÁRIO:

Realiza as transações funcionais exigidas pela aplicação. Ele é composto pelos programas de aplicação.

Concluindo, a filosofia de descentralização plena adotada no projeto do centro de supervisão, possibilitou que a VGI fosse construída de modo a assegurar uma comunicação confiável, econômica e de banda passante adequada às reais necessidades de transmissão de dados entre operadores.

III.3.2.3 SUBSISTEMA DE OBSERVAÇÃO E SALVAMENTO (SOS)

É o conjunto de técnicas de "hardware e "software" utilizadas para aumentar o grau de observabilidade e a disponibilidade do centro de supervisão e controle.

O SOS não visa apenas o aspecto de detecção e recuperação de falhas. Ele tem também como objetivo a observação de todo o

estado operacional do sistema, permitindo aos usuários completa visibilidade do mesmo.

O subsistema de observação e salvamento será alvo de análises detalhadas nos próximos capítulos deste trabalho. A seguir damos uma breve descrição das partes que o compõem.

i - Observação interna do operador: consiste de mecanismos que realizam a observação interna do operador, examinando sua CPU, interfaces e periféricos;

ii - Observação do sistema: composto de mecanismos que permitem a observação do estado de funcionamento do sistema de supervisão. Analisa o comportamento de cada módulo básico a partir das saídas por ele produzidas;

iii - Reconfiguração do sistema: tem como objetivo alterar a configuração do sistema para isolar módulos ou periféricos defeituosos, coordenando a degradação do sistema dentro de uma estratégia ótima;

iv - Recuperação dos elementos básicos: recursos para manutenção "on-line" do sistema. Esta manutenção pode ser automática ou manual, colocando-se módulos sobressalentes ou colocando-se à disposição da equipe de manutenção uma série de facilidades para a rápida localização e substituição de elementos defeituosos;

III.3.2.4 UTILITÁRIOS

Os utilitários representam o conjunto de ferramentas que fazem com que o desenvolvimento dos programas de aplicação seja o mais confortável possível. Para isto é necessário que o

usuário (programas de aplicação) possa se abstrair de detalhes do projeto do sistema básico e tenha a sua disposição ferramentas tais como: manipuladores de tabelas, listas, etc.

Os utilitários previstos para o sistema podem ser agrupados segundo as classes abaixo:

i - Processadores de entrada e saída para periféricos tais como:

- Teclado, vídeo, impressora, registrador gráfico, painel mímico, terminais remotos, etc.

ii - Manipuladores de estruturas de dados tais como :

- Gerenciador do esquema físico: responsável pela operações elementares sobre registros (modificação, deleção, inserção, localização, etc.);

- Gerenciador do esquema conceitual: a partir da definição da estrutura de dados, gerencia todas as operações de obtenção e modificação dos dados;

- Gerenciador das imagens da base de dados para as diversas aplicações: reponsável pelos pedidos de dados ao gerenciador do esquema conceitual e colocação destes dados da forma que se deseja utilizá-los (forma específica de utilização).

iii - Rotinas de cálculo:

- Envolve toda a biblioteca de rotinas de cálculo disponíveis na linguagem de programação adotada, bem como rotinas específicas desenvolvidas ao longo do projeto.

iv - Coordenadores da consistência do banco de dados replicado:

- Envolvem todas as primitivas utilizadas para a

inicialização e alteração do banco de dados, levando em conta a existência de um sistema redundante. Esta consistência será realizada através de coordenadores que sincronizarão os pedidos de alteração do banco de dados.

III.3.2.5 SUPORTE OFF-LINE (SOF)

O SOF consiste de um conjunto de técnicas e ferramentas para:

- Desenvolvimento de programas e textos que compreende: edição de textos, compilação de programas, utilitários de "linkedição", localização, conversão para código executável nos operadores do sistema, além de fornecer ferramentas para a realização de "back-up" dos arquivos de programas e dados;

- Suporte de depuração: envolve utilitários diversos para depuração "off-line" e "on-line" de programas.

- Edição e compilação da base de dados: consiste no editor de diagramas unifilares, tabelas, esquema relacional e compilador do banco de dados dos diversos operadores.

III.4 DESCRIÇÃO FUNCIONAL DO CENTRO DE SUPERVISÃO

A figura (III.8) apresenta a configuração básica do centro de supervisão e controle desenvolvido pelo CEPEL. Nele podemos ver as três partes que compõem um centro de supervisão: subsistema de comunicação, subsistema de supervisão e controle "on-line" e subsistema de suporte "off-line".

III.4.1 SUBSISTEMA DE COMUNICAÇÃO

A operação do COR depende fundamentalmente dos dados que são coletados do sistema sob controle, pois as decisões que são tomadas pelos operadores do sistema elétrico (despachante) baseiam-se nestes dados.

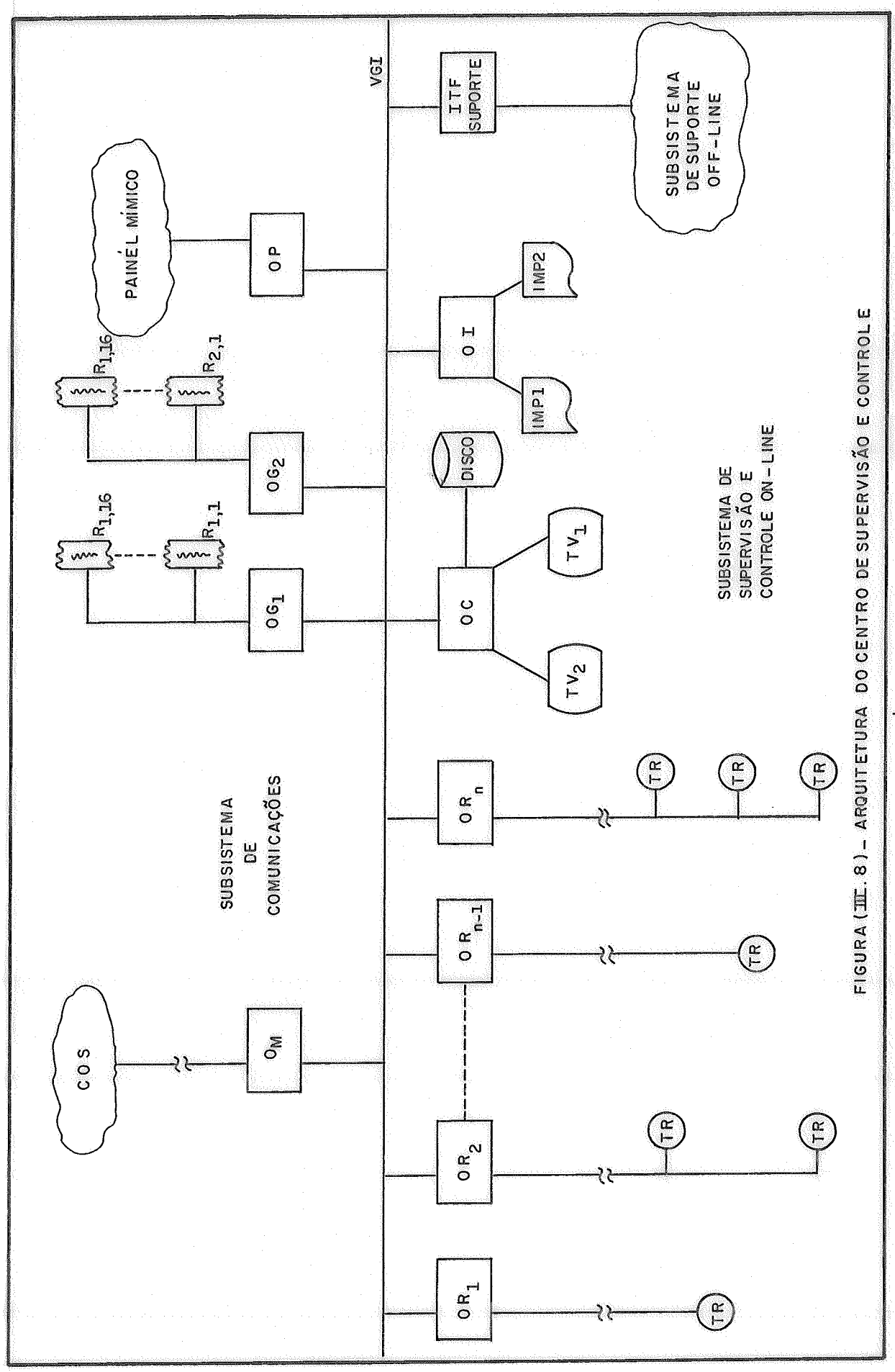


FIGURA (III. 8) - ARQUITETURA DO CENTRO DE SUPERVISÃO E CONTROLE

Um centro de supervisão e controle para sistemas elétricos geralmente supervisiona as seguintes grandezas (19):

i - Grandezas digitais

Estas grandezas supervisionadas estão associadas com o estado (binário: aberto ou fechado) de determinados dispositivos como: chaves seccionadoras, disjuntores e relés de proteção;

ii - Grandezas analógicas

São grandezas que representam o valor de uma variável analógica: tensão, corrente, potência ativa e reativa.

iii - Grandezas de acumulação

São contadores que acumulam o número de pulsos emitidos por certos dispositivos, cuja finalidade é medição de energia com o objetivo de faturamento.

O subsistema de comunicação é composto de dois tipos de operadores: Operador de Master e Operador de Remota.

As principais funções de um operador de remota são;

i - Coordenar a comunicação com os terminais remotos instalados junto aos processos, recebendo destes as informações necessárias à criação de uma base de dados dinâmica com o estado corrente do sistema supervisionado;

ii - Transmitir aos terminais remotos as ordens de controle.

A comunicação com os terminais remotos se processa basicamente de uma forma radial, isto é, existirá um canal de comunicações, um MODEM e um operador dedicados a cada remota. Excepcionalmente, mais de um terminal remoto (no máximo três)

podem compartilhar um mesmo canal de comunicações e conseqüentemente o mesmo operador da remota. Um operador de remota é constituído de um módulo básico mais um módulo de interface com o MODEM de 1200 bps.

Existem funções no COS (despacho central) que dependem das informações atualizadas disponíveis no COR, devendo este providenciar que as informações coletadas nos diversos terminais remotos cheguem até o COS. Para realização desta função, e de outras, utilizou-se um operador chamado Operador de Master cujas funções são (20):

i - Comunicação com o COS;

ii - Coletar nos demais operadores as informações a serem transmitidas ao COS;

iii - Distribuição, para os operadores do COR, das informações recebidas do COS.

O operador de MASTER é composto de um módulo básico e uma interface para MODEM de 4800 bps.

III.4.2 SUBSISTEMA DE SUPERVISÃO E CONTROLE "ON-LINE".

O subsistema de supervisão e controle on-line, também chamado de Interface Homem Máquina (IHM) é a parte do sistema responsável pela realização da comunicação entre o despachante e o sistema computacional.

A IHM é composta pelos seguintes operadores: operador de console (OC), operador de impressão (OI), operador de registradores gráficos (OG) e operador de animação do painel mímico (OP).

i - Ao OC cabe o desempenho das principais funções de interface homem-máquina como: apresentação dos diagramas da rede elétrica, apresentação de tabela, emissão de alarme, atendimento do controle digitado pelo

despachante, etc.

O OC é constituído de um módulo básico, módulos de expansão de memória e dos seguintes periféricos:

- Dois CRT semigráficos à cores;

- Um teclado alfanumérico, dotado de símbolos gráficos especiais e teclas de funções especiais;

- Uma unidade de memória de massa, disco do tipo WINCHESTER, com capacidade de 5 Mbytes;

- Uma unidade de entrada e saída por disco flexível.

ii - O OI é constituído de um módulo básico e duas impressoras. Ele receberá dos outros operadores as mensagens a serem impressas e as distribuirá entre as impressoras.

As duas impressoras estão destinadas uma a impressão de relatórios outra para registro de alarmes.

iii - Para atender às funções de registros gráficos a IHM contém dois OGs, tendo cada OG a capacidade de controlar até 32 registradores. Opcionalmente, poderá estar associado a cada registrador gráfico um mostrador digital ("displays" de sete segmentos) com quatro algarismos e ponto decimal, capaz de apresentar o valor instantâneo da grandeza em registro.

iv - O OP está destinado à animação do painel mímico, que é um painel que contém um esquema simplificado da rede elétrica que está sendo supervisionada pelo COR.

Em função dos dados existentes nos diversos ORs, o OP controlará o acendimento de lâmpadas no painel, que indicarão aos despachantes a existência de algum evento naquele ponto da rede.

III.4.3 SUBSISTEMA DE SUPORTE E DESENVOLVIMENTO

O subsistema de suporte e desenvolvimento proverá recursos para:

- Manutenção da base de dados;
- Manutenção de telas do CRT;
- Desenvolvimento de novos programas.

Além de um sistema hospedeiro onde são executados os utilitários para realização das funções acima, este subsistema é dotado de um conjunto de operadores idênticos aqueles do COR, possibilitando a realização de testes nos produtos em desenvolvimento. Foram também desenvolvidos simuladores de COS e de terminal remoto que podem gerar dados para excitarem estes programas.

Uma vez gerados e testados, os novos arquivos são transferidos para a memória de massa do OC, onde ficam disponíveis para os testes finais, em ambiente real, para serem integrados ao sistema.

III.5 - AVALIAÇÃO DA DISPONIBILIDADE DO SISTEMA SEM TÉCNICAS DE TOLERÂNCIA A FALHAS

Concluindo a apresentação do Centro de Supervisão, faremos neste capítulo um estudo da taxa de falhas e da disponibilidade do sistema, mostrando a necessidade de introdução de técnicas de tolerância a falhas.

III.5.1 - O CONCEITO DE DISPONIBILIDADE

Tradicionalmente, ao se calcular a disponibilidade de um sistema, considera-se que todos os elementos deste estão em série. A falha de qualquer um destes elementos provoca a paralisação do sistema. Entretanto, no caso do nosso sistema há uma certa redundância nas informações apresentadas ao operador, além do sistema ser distribuído. Assim, serão levados em

consideração, para o cálculo da disponibilidade, apenas algumas partes do sistema.

Do ponto de vista do usuário, um operador do sistema elétrico (despachante), a disponibilidade do Centro de Supervisão é a probabilidade de que a rede elétrica possa ser observada e controlada, em um instante de tempo t (7). Na arquitetura proposta para o centro, para assegurar esta capacidade de observar e controlar a rede elétrica, temos que garantir a execução das funções de: acompanhamento de todas as variáveis, alarmes, relatórios e comunicação com o COS. Para isto devemos ter em perfeito estado de funcionamento os seguintes elementos pertencentes aos diversos subsitemas:

- Console;
- Impressoras;
- Via Geral de Interconexão;
- Comunicação com o COS;
- Comunicação com as remotas;
- Fontes de alimentação.

Ou seja, a disponibilidade do COR é dada por:

$$A = A1.A2.....Ai$$

onde: Ai = disponibilidade do elemento i.

III.5.2 - PREVISÃO DA TAXA DE FALHAS

A determinação da taxa de falhas de um equipamento, na fase de projeto, não pode ser feita com precisão, pois muitos são os fatores que influenciam esta taxa. Geralmente, é feita uma previsão com o objetivo de se estudar e propor técnicas que melhorem a qualidade do sistema.

Esta previsão é feita com base em um pequeno conhecimento do comportamento do sistema, com a finalidade de se criar uma base de dados indispensável ao desenvolvimento de um modelo para o sistema. O processo completo consiste em prever, propor

novas técnicas, medir (ou ganhar mais experiência), novamente prever, propor mais técnicas e medir continuamente por todo um programa de desenvolvimento e pesquisa.

O nosso trabalho nesta seção consistirá numa previsão preliminar. No nosso ponto de vista, consideramos que esta previsão é útil não só para se ter uma idéia da qualidade do equipamento, mas também para mostrar se uma arquitetura é melhor (mais confiável) que outra, se a introdução de uma determinada técnica irá introduzir ou não algum benefício no sistema.

Para se fazer a estimativa da taxa de falhas dos componentes utilizamos o modelo mais largamente empregado: as normas MIL-HDBK-217C (21).

Para os componentes de que possuíamos todos os dados foi usado o modelo completo. Para aqueles onde não foi possível levantar todos os dados usamos a taxa de falhas genérica proposta pelas normas. E, finalmente, para aqueles componentes onde foi impossível obter algum dado, decidimos adotar a taxa de falhas de um outro componente, cujo valor fosse seguramente maior ou igual ao do componente desconhecido.

No anexo I pode-se encontrar maiores detalhes sobre a taxa de falha de todos os componentes usados na construção do Centro de Supervisão.

III.5.3 - AVALIAÇÃO DA DISPONIBILIDADE

A disponibilidade de um sistema sem redundâncias é expressa por:

$$A = \Psi / (\lambda + \Psi)$$

λ = taxa de falhas do sistema

Ψ = taxa de manutenção

Para calcular a taxa de falhas do sistema consideramos que todos os elementos vitais do sistema estão em série. Assim, a taxa de falhas total é a soma das taxas de falhas de todos os componentes.

$$\lambda = \sum_{1}^{n} N_i \cdot \lambda_i$$

N_i = número de componente do tipo i;
λ_i = taxa de falhas do componente i.

Para a configuração abaixo obtivemos a disponibilidade do sistema de 97,57%.

A tabela (III.1) mostra a disponibilidade dos diversos elementos.

ELEMENTOS	TAXA DE FALHAS/Mh	DISPONIBILIDADE
OM	150	99,85%
OR	100 (x16)	98,43%
OC	450	99,55%
OI	250	99,75%
FONTES	2 x 7	99,99%
VGI	0,87 x 20	99,98%
TOTAL	2483	97,57%

Tabela (III.1) - Disponibilidade do sistema simplex

Para realização desta tabela foram usados os seguintes valores:

- TF de um módulo básico = 50 f/Mh;
- TF de um operador de console = 150 f/Mh;
- TF de um modem 1200 bps = 50 f/Mh;
- TF de um periérico = 100 f/Mh;
- TF da fonte de alimentação = 2 f/Mh;
- TF da VGI = 0,87 f/Mh;
- tempo médio de manutenção de 10 horas, considerado razoável em FURNAS, já que durante o periodo noturno não há equipe de manutenção no COR. Este tempo equivale a uma taxa de manutenção de 100.000 /Mh.

Obs: TF = taxa de falhas;
Mh = um milhão de horas.

III.6 - CONCLUSÃO

Podemos ver que para uma configuração média o Centro de Supervisão não atende às especificações exigidas, que é uma disponibilidade de 99,8%. Assim, algumas medidas devem ser tomadas para que se consiga a disponibilidade desejada.

No próximo capítulo estudaremos as técnicas sugeridas para melhorar a disponibilidade do sistema.

CAPÍTULO IV

SUBSISTEMA DE OBSERVAÇÃO E SALVAMENTO

IV.1 - INTRODUÇÃO

O Sistema de Observação e Salvamento (SOS), proposto a seguir, é um conjunto de técnicas responsável por detectar a ocorrência de uma falha, recuperar o sistema desta falha e reconduzi-lo a seu estado normal de funcionamento. Além disso, o SOS tem a função de observar o estado operacional do Centro de Supervisão e Controle, permitindo aos usuários uma completa visibilidade do mesmo. O SOS pode ser visto como um Sistema de Supervisão e Controle do próprio Centro de Supervisão e Controle.

IV.2 - CARACTERIZAÇÃO DAS FALHAS A SEREM TOLERADAS

O passo inicial para introduzir no sistema técnicas de tolerância a falhas é caracterizar o conjunto das falhas que se deseja tolerar.

Para tanto deve-se primeiro especificar o grau de modularização do sistema quanto à tolerância a falhas. Esta decisão é muito importante, pois é neste ponto que se escolhe o nível onde as técnicas de tolerância a falhas serão empregadas (nível interno aos integrados, nível de pino de integrado, nível de integrado, conjunto de integrados ou a nível do próprio sistema).

As primeiras dúvidas que podem surgir são, por exemplo: qual a necessidade de se dividir o sistema em módulos? Por que não fazer o sistema inteiro redundante? Por que colocar redundâncias a nível de módulo? Para responder estas perguntas vamos analisar dois sistemas equivalentes (com a mesma taxa de falhas). No primeiro, o sistema inteiro é redundante. No segundo, a redundância foi feita a nível de módulo.

A disponibilidade dos dois sistemas é dada por:

$$D1 = \psi(3n\lambda + \psi)/((2n\lambda + \psi).(n\lambda + \psi))$$

$$D2 = ((\psi(3\lambda + \psi) / ((2\lambda + \psi).(\lambda + \psi))) ** n$$

D1 - disponibilidade do sistema todo duplicado;

D2 - disponibilidade do sistema duplicado por módulo;

λ - taxa de falhas de cada módulo (50 f/Mh);

ψ - taxa de manutenção (100.000/Mh);

n - número de módulos;

$n\lambda$ - taxa de falhas do sistema todo.

OBS.: Mh = 1 milhão de Horas.
Foi suposto que todas as falhas são reparadas simultanea ente.

Usando valores típicos do nosso sistema obtemos a tabela (IV.1), que mostra a disponibilidade dos dois sistemas para diversos valores de n.

Da tabela (IV.1) vemos que a redundância a nível de módulo é mais vantajosa. Isto é fácil de se visualizar, pois no primeiro sistema, após a ocorrência da primeira falha, todo o sistema é substituído, não havendo mais redundâncias disponíveis. Entretanto, no segundo caso mesmo que haja mais de uma falha, se estas ocorrerem em módulos diferentes o sistema continuará operando. Em ambos os casos considerou-se desprezíveis as taxas de falhas dos elementos de comutação dos módulos redundantes.

Em alguns sistemas a divisão por módulo não é muito simples, porém, no nosso sistema esta divisão é natural, já que

um dos parâmetros importantes na concepção do projeto foi justamente a modularidade. Assim, neste caso, podemos definir o módulo relativo às técnicas de tolerância a falhas, como sendo o próprio Operador Básico (módulo básico + periféricos).

N	D1 (%)	D2 (%)
2	99,99980	99,99990
3	99,99955	99,99985
4	99,99920	99,99980
5	99,99876	99,99975
6	99,99822	99,99970
7	99,99758	99,99965
8	99,99684	99,99960
9	99,99600	99,99955
10	99,99507	99,99950

Tabela (IV.1) - Disponibilidade de sistemas duplicados e duplicados por módulos.

IV.2.1 - CARACTERIZAÇÃO DOS ERROS PRODUZIDOS POR UMA FALHA EM UM MÓDULO.

Como foi visto no item anterior a nossa unidade de trabalho (módulo) é um Operador Básico. Qualquer falha permanente no interior deste, eliminará aquele módulo do sistema. Isto porque nenhuma redundância será colocada no interior do módulo. Dentro de cada um deles colocaremos apenas dispositivos para detectar e recuperar falhas transientes.

Todas redundâncias serão colocadas a nível de módulos.

Do ponto de vista do sistema, uma falha num determinado módulo só poderá produzir algum efeito (erro) no sistema através de suas interfaces de entrada e saída.

A figura (IV.1) apresenta os dois tipos de interface de entrada e saída que um módulo pode apresentar:

i - interface de interligação com a rede interna de comunicação;

ii - interface de interligação do módulo básico com o periférico específico daquele operador.

Os erros que um módulo pode apresentar ao sistema são:

i - O módulo não produz sinal em algumas de suas interfaces;

ii - O módulo produz um sinal intermitente;

iii - O módulo produz um sinal, porém de conteúdo semântico errado.

Qualquer falha que produza um dos três erros acima deverá disparar os mecanismos de detecção e recuperação.

Quanto às falhas transientes, estas merecem um tratamento especial. A ocorrência de uma falha transiente não deve provocar a substituição do módulo, pois, após cessarem os efeitos de uma falha deste tipo, o módulo afetado pode continuar sua operação normal. Não seria inteligente gastar os recursos de redundância substituindo módulos que ainda possuem capacidade de operação. Logo, serão criados também mecanismos especiais de detecção de falha e recuperação do módulo, que, além de analisarem o funcionamento das interfaces do módulo observam também o estado interno de cada módulo.

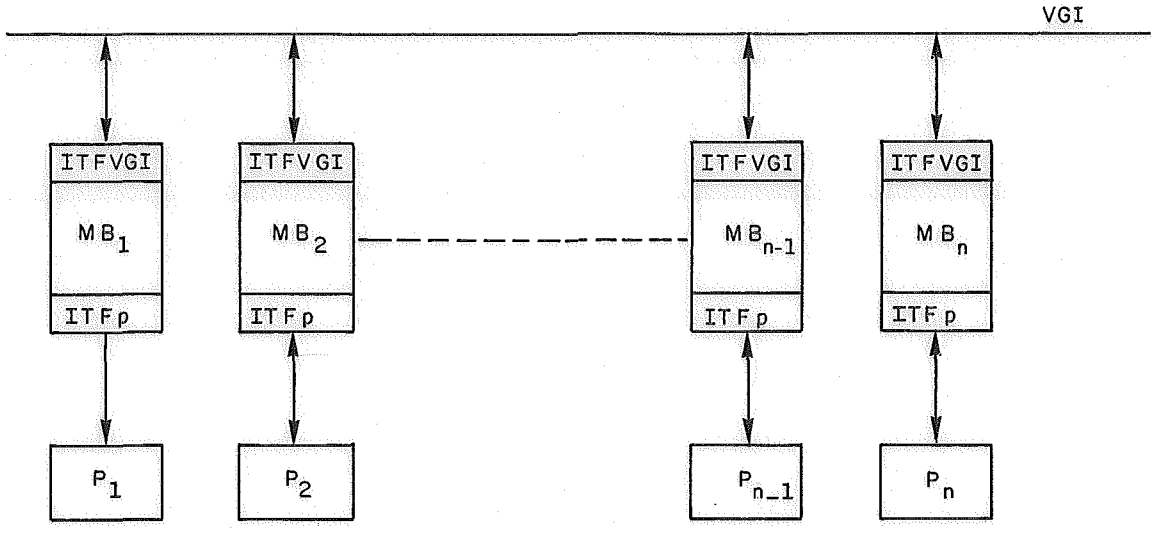


FIGURA (IV . 1) – TIPOS DE INTERFACES DE UM MÓDULO BÁSICO (MB)

IV.2.2 - METODOLOGIA DE OBSERVAÇÃO (DETECÇÃO).

Pelo que foi exposto anteriormente podemos distingüir dois níveis de observação:

i - Mecanismos internos ao módulo - São mecanismos, tanto de "hardware" quanto de "software", que são incorporados ao módulo com função de detectar uma falha e recuperar o módulo;

ii - Mecanismos externos ao módulo - Estes mecanismos têm acesso ao estado do módulo somente através dos sinais produzidos por ele nas suas interfaces.

A diferença entre estes mecanismos, além de sua posição em relação ao módulo, é seu tempo de atuação. Os mecanismos internos são mais rápidos e assumem sempre que uma falha detectada é transiente, acionando os dispositivos de recuperação de falhas transientes (restauração de base de dados, carga de programa, etc.).

Os mecanismos externos esperam um tempo maior antes de atuarem. Assim, se a falha for transiente, os dispositivos internos de recuperação reconduzem o operador a seu estado normal. Caso esta recuperação não se efetive, os mecanismos externos acionarão os dispositivos de reconfiguração do sistema.

Nos próximos ítens estudaremos estes mecanismos mais detalhadamente.

IV.3 - FUNÇÕES DO SUBSISTEMA DE OBSERVAÇÃO E SALVAMENTO

O SOS tem por objetivo as seguintes funções.

- Observar cada módulo internamente;
- Observar o sistema globalmente;
- Ter capacidade de reconfigurar o sistema;

- Ter recursos que permitam ao sistema ser tolerante a falhas.

As figuras (IV.2), (IV.3), (IV.4), (IV.5) e (IV.6) apresentam em Linguagem de Módulos Estruturados (LME) as funções que o SOS deve apresentar.

IV.3.1. OBSERVAÇÃO INTERNA DO MÓDULO

Consiste de mecanismos de observação interna de cada operador (CPU + Interfaces + Periféricos).

Entradas

i - Falha a nível de módulo , como por exemplo: Erro de paridade, violação de memória, etc.;

ii - Comandos ou eventos externos - são qualquer tipo de estímulos externos.

Controle

- Como controle para esta função temos os limites que são valores pré-definidos sobre as características de funcionamento do módulo.

Mecanismos

i - Internos - são dispositivos incorporados internamente ao módulo que realizam a observação do módulo (ex: gerador de paridade, proteção de memória, etc.);

ii - Externos: são mecanismos que permitem ao operador humano observar o módulo;

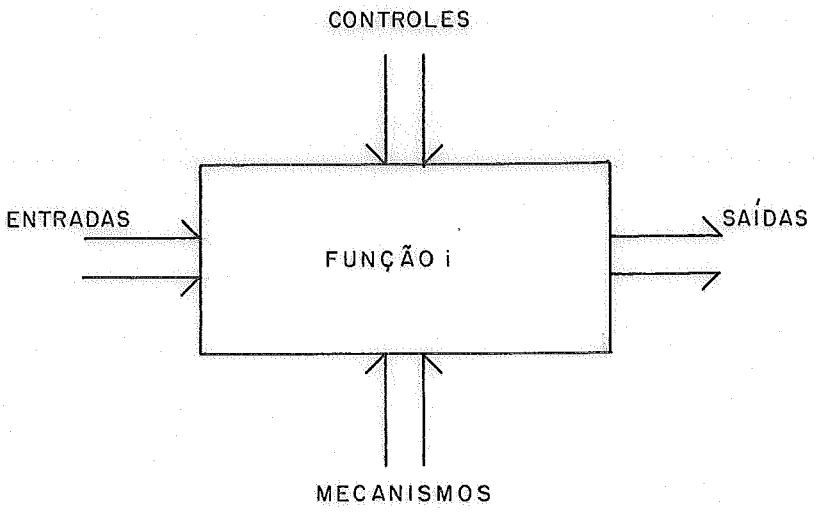


FIGURA (IV.2) - LINGUAGEM DE MÓDULOS ESTRUTURADOS(LME)

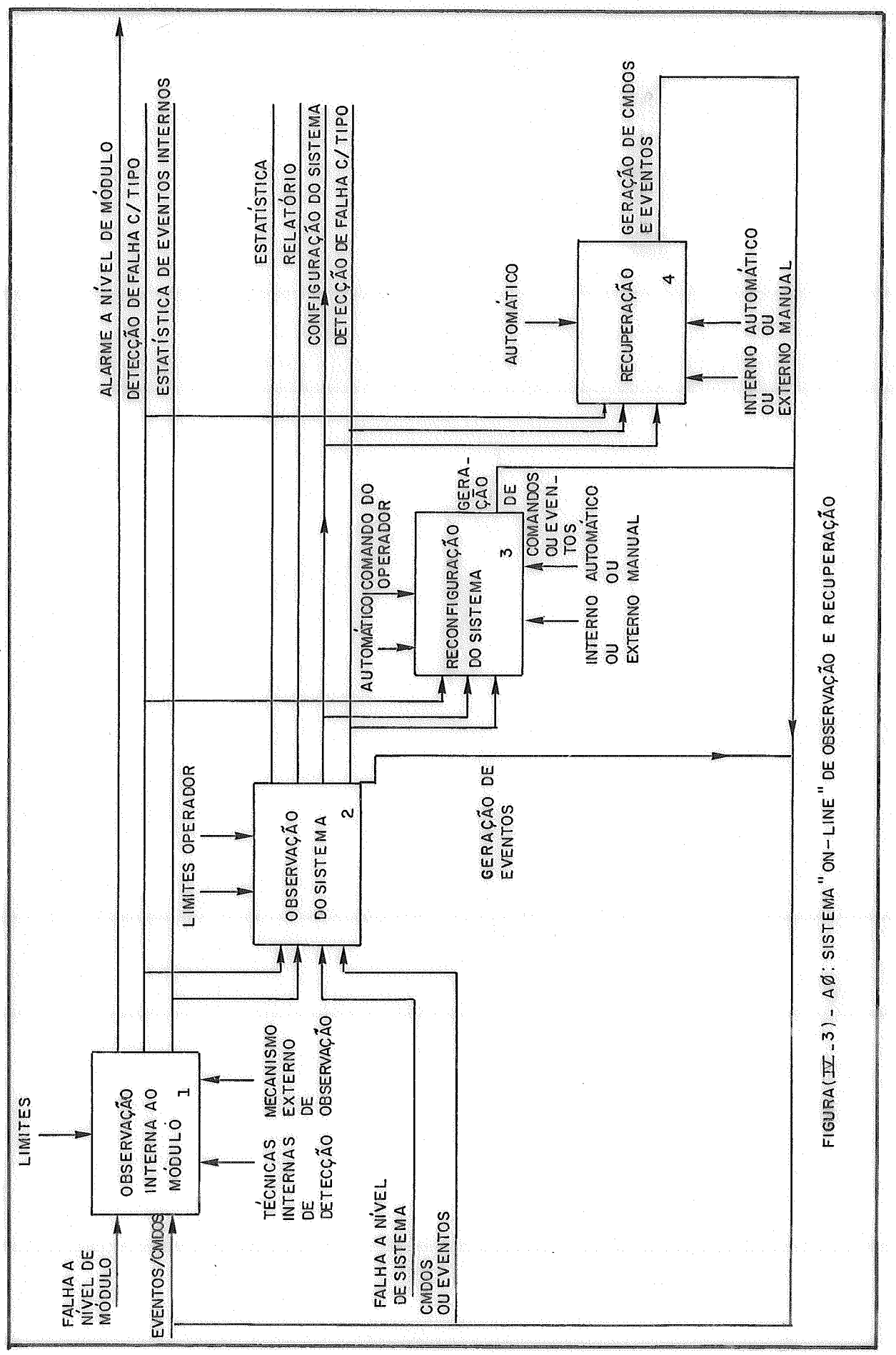


FIGURA (IV - 3) - AØ: SISTEMA "ON-LINE" DE OBSERVAÇÃO E RECUPERAÇÃO

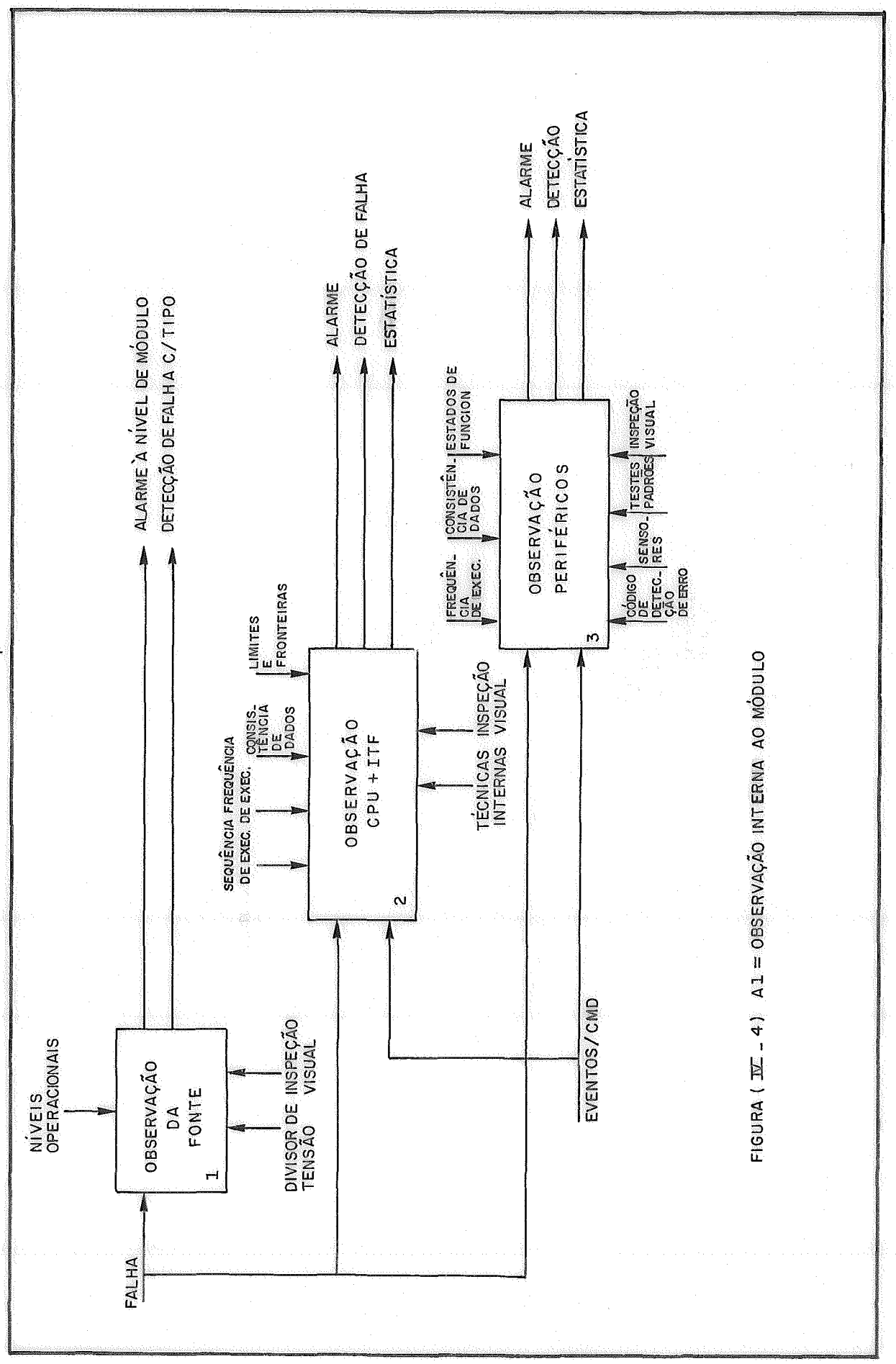


FIGURA (IV - 4) A1 = OBSERVAÇÃO INTERNA AO MÓDULO

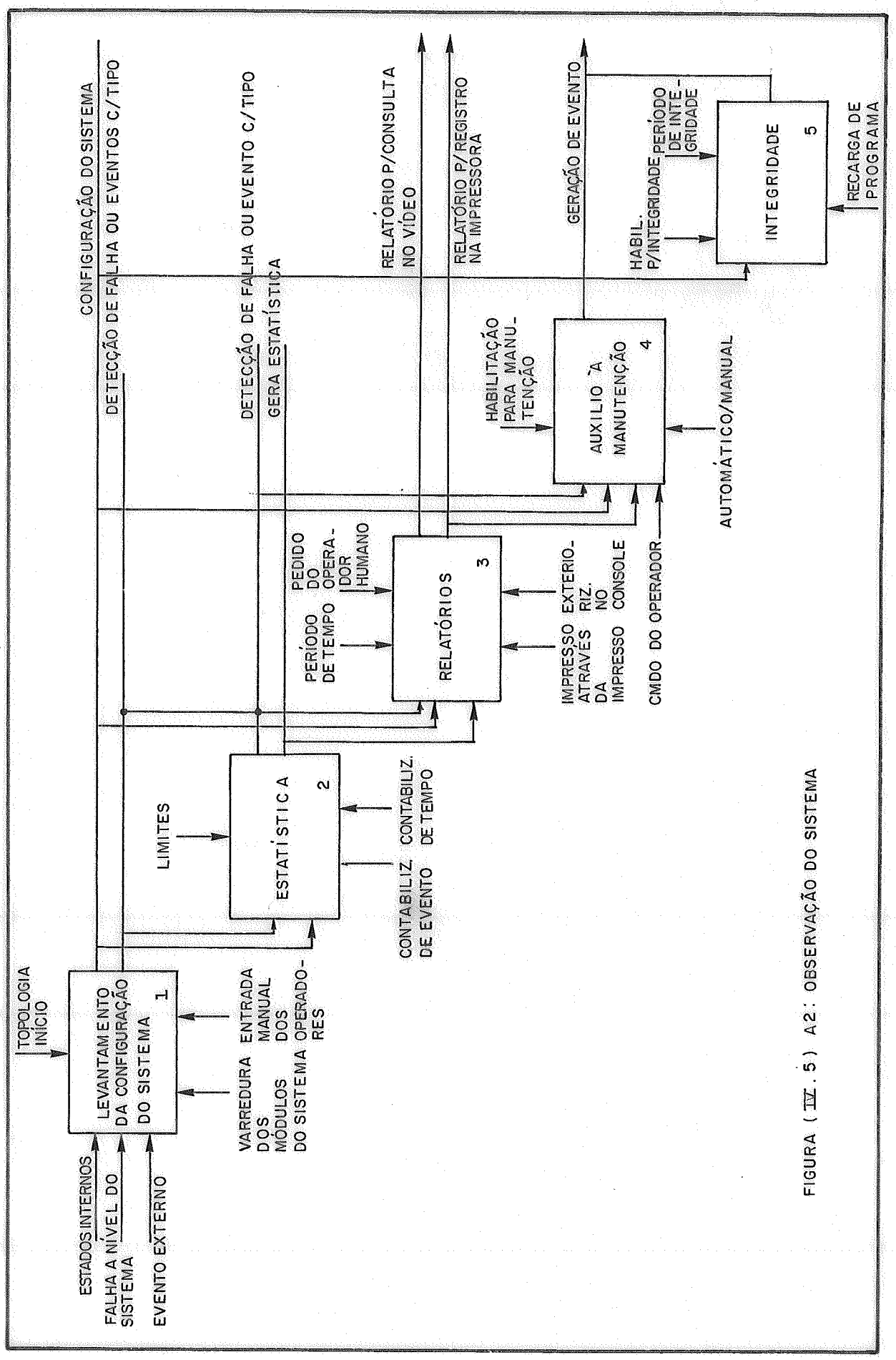


FIGURA (IV . 5) A2: OBSERVAÇÃO DO SISTEMA

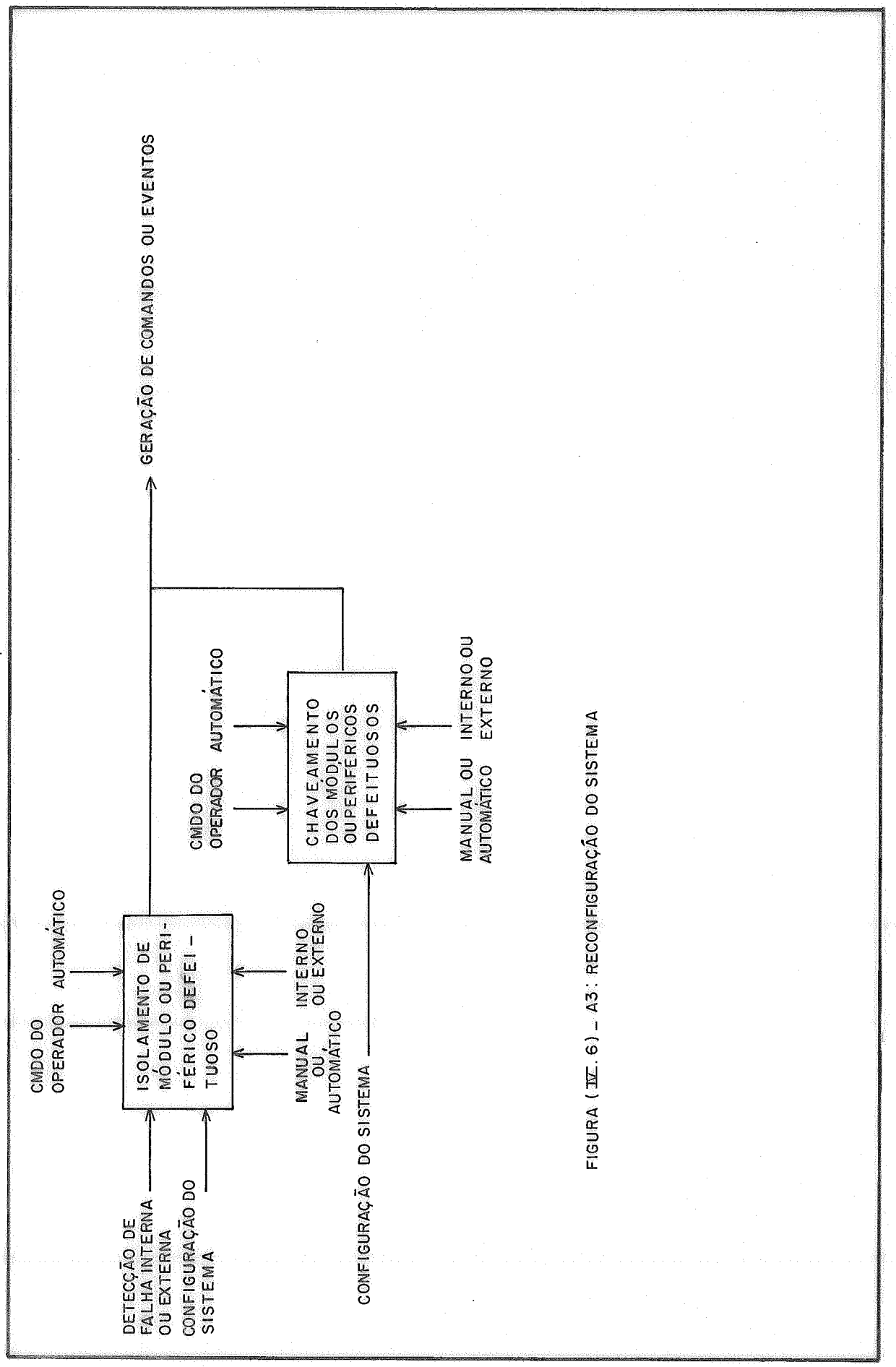


FIGURA (IV. 6) - A3: RECONFIGURAÇÃO DO SISTEMA

Saídas

i - Alarmes a nível de módulos - são saídas que permitem ao operador humano observar o estado de funcionamento do módulo (ex: painel);

ii - Detecção de falha - são saídas que permitem ao sistema observar o estado de funcionamento do módulo;

iii - Estatística de eventos internos - são saídas que indicam o valor das acumulações dos eventos internos (ex: contadores de eventos periódicos, contadores de erros nas comunicações).

Podemos ainda subdividir a função de observação interna nas seguintes partes (como mostra a figura (IV.4)):

- observação das fontes;
- observação da cpu + interface;
- observação dos periféricos.

IV.3.2 FUNÇÃO DE OBSERVAÇÃO DO SISTEMA

Permite a observação do estado de funcionamento do sistema, analisando o estado de funcionamento de cada módulo a partir de suas saídas.

Entradas

i - Detecção de falha interna aos módulos;
ii - Estatísticas de eventos internos;
iii - Comandos/eventos externos;
iv - Falha a nível de sistema - são falhas que podem ser observadas por outro módulo (ex:"time-out" na VGI, dados ou comandos errados).

Controles

i - Limites previamente estabelecidos sobre o funcionamento

do sistema ou de cada módulo;

ii - Comandos do operador.

Saídas

i - Estatísticas sobre o funcionamento do sistema (ex: taxa de erros de comunicação, número de reinicializações, etc.);

ii - Relatório - exteriorização do resultado das estatísticas, testes, registro de eventos, etc.;

iii - Configuração do sistema - é o resultado do estado de funcionamento do sistema;

iv - Detecção de falhas - detecção a nível de sistema das falhas existentes.

Como mostra a figura (IV.5), podemos dividir esta função nas seguintes partes:

i - Levantamento da configuração do sistema;

ii - Estatística;

iii - Relatórios;

iv - Auxílio à manutenção - são procedimentos que auxiliam a equipe de manutenção na detecção, localização e reparo de defeitos;

v - Integridade - é um mecanismo que garante a integridade dos dados e programas nos diversos módulos do sistema.

IV.3.3 RECONFIGURAÇÃO DO SISTEMA

Esta função tem como objetivo alterar a configuração do sistema para substituir módulos ou periféricos defeituosos,

chaveando módulos sobressalentes no lugar dos defeituosos. Para cada subsistema deve-se estudar a maneira mais conveniente de se colocar as redundâncias, dependendo das particularidades de cada um.

Entradas

i - detecção de falhas internas aos módulos;
ii - detecção de falhas à nível do sistema;
iii - configuração do sistema;

Controle

i - automático;
ii - comandos do operador;

Mecanismos

i - internos ou externos (ex: detecção de módulos defeituosos, chaveamento, etc.);

ii - automático ou manual (ex: chaveamento automático, extração ou inserção de um módulo.);

Saída

i - geração de comandos ou eventos que produzirão a reconfiguração do sistema.

IV.3.4 RECUPERAÇÃO

Esta função consiste nos dispositivos, algoritmos, etc., para reconduzir o sistema ao seu estado normal de funcionamento. Esta recuperação pode ser automática, chaveando-se módulos sobressalentes, carregando-se programas, isolando-se módulos defeituosos, etc., ou manual, sendo necessária a participação do operador.

Entradas

i - detecção de falhas internas ao módulo;
ii - configuração do sistema;
iii - detecção de falhas a nível do sistema.

Controle

i - Automático;

Mecanismos

i - Internos ou externos;
ii - automáticos ou manuais;

Saída

i - Geração de comandos/eventos que disparem os mecanismos de recuperação.

IV.4 - DESCRIÇÃO DOS PRINCIPAIS MECANISMOS DESENVOLVIDOS

Os principais mecanismos desenvolvidos para atender as especificações mostradas na seção anterior são descritos a seguir.

IV.4.1 - MECANISMOS DE OBSERVAÇÃO DO MÓDULO

IV.4.1.1 - PROTEÇÃO DE MEMÓRIA

Esta técnica baseia-se na proteção de determinadas áreas de memória contra acessos indevidos. Por exemplo, pode-se proteger contra escrita regiões de memória destinadas a armazenar programas.

Existem computadores, mais sofisticados, que controlam todos os acesso à memória permitindo que cada processo ("JOB") tenha acesso apenas a uma pequena janela da memória (área de trabalho). Caso seja feito um acesso fora desta janela ou se tente fazer uma escrita em uma região de código, o

processamento é interrompido e a rotina de auto diagnóstico tomará as medidas necessárias para a restauração do processamento normal.

No nosso caso a proteção de memória é mais simples. O principal objetivo dela é detectar a tentativa de uma escrita em uma região de código de programas.

A figura (IV.7) apresenta o circuito da proteção de memória. Ele consiste de um registro onde, na inicialização de programa, escreve-se o endereço da fronteira entre a região protegida e a região livre. Um comparador compara constantemente o valor corrente da Barra de endereço do microprocessador com o valor armazenado no registro, gerando um sinal de maior, menor ou igual. Combinando-se um destes sinais com o sinal de escrita em memória gera-se um sinal de erro, que significa uma tentativa de escrita numa região protegida de memória.

Esta técnica é importante não só para garantir a integridade de programas e base de dados, mas também na detecção da perda de sequência de processamento, pois a probabilidade de um programa perdido acessar uma posição de memória fora da área de dados é muito grande.

IV.4.1.2 - CÓDIGO DE DETECÇÃO DE ERRO NA MEMÓRIA

Como pode ser observado no anexo I, a memória de um módulo é responsável por mais de 50% da taxa de falhas permanentes, além dela também ser responsável por um grande número de falhas transientes. Assim, é muito comum, em quase todos os sistemas encontrados, a utilização de códigos de detecção de erros em memória para garantir a integridade dos dados armazenados nela, principalmente nas memórias do tipo leitura e escrita (RAM).

Os códigos de detecção de erro mais comumente encontrados nas memórias principais baseiam-se no código de Hamming para correção de apenas um erro. Os códigos do tipo BCH (BOSE, CHAUDHURI e HOCQUENGHEM), usados para correção de erros

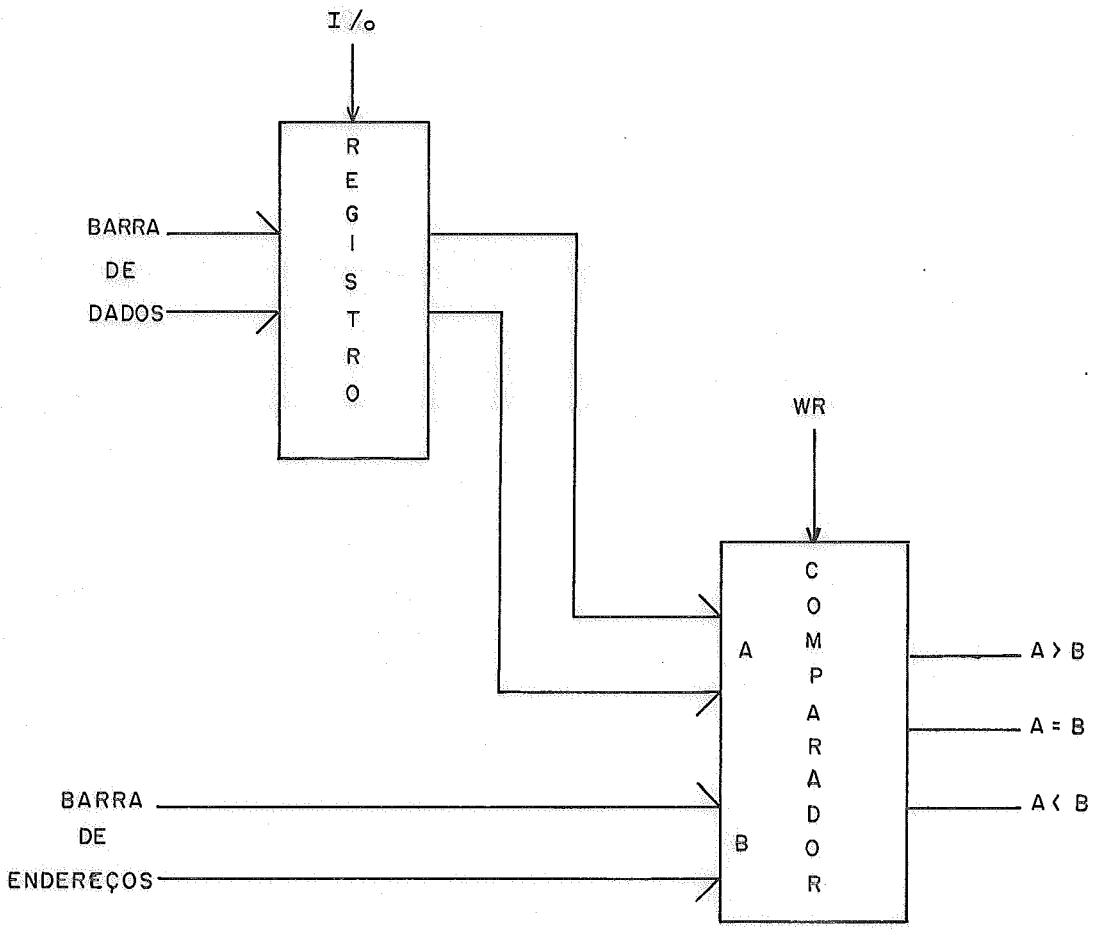


FIGURA (IV.7) – ESQUEMA DA PROTEÇÃO DE MEMÓRIA

múltiplos, são muito complexos e geralmente não são usados em memórias de semicondutores.

A correção de um erro e a detecção de até dois "bits" errados são obtidas colocando-se redundâncias na informação armazenada na memória. A figura (IV.8) apresenta um esquema para correção de um erro simples e detecção de um erro duplo. Um campo com k "bits" de paridade é gerado a partir de m "bits" de dados, sendo ambos armazenados na memória. O número total de "bits" armazenados é igual a k + m. Durante o ciclo de leitura são gerados novamente k "bits" de paridade, que são comparados com os k "bits" que foram armazenados na memória anteriormente. Se o resultado for diferente é gerado um sinal de erro para um mecanismo de correção.

A organização física dos componentes de memória é importante para melhorar a eficiência dos códigos de detecção e correção de erros. AS RAMS devem ser arranjadas de tal modo que a cada circuito integrado de memória corresponda apenas um "bit" da palavra de memória. Este arranjo garante que uma falha em um integrado produza apenas um erro por palavra. Entretanto, para memórias pequenas geralmente não se usa correção de erro. Um "bit" de paridade por,"byte" de informação é mais do que suficiente. Para memória de 256 K x 64 "bits" costuma-se usar mecanismos mais sofisticados de detecção e correção de erro.

O dispositivo para detecção de erro na memória foi implementado para detectar a ocorrência de apenas um "bit" errado, não sendo desenvolvido a parte relativa a correção do erro detectado.

IV.4.1.3 - MECANISMOS ESPECIAIS DE OBSERVAÇÃO INTERNA DOS MÓDULOS

Estes mecanismos tem o objetivo de melhorar, de um modo geral, o grau de observação interna do módulo e a localização de falhas. Estes mecanismos não possuem, como os que foram descritos anteriormente, ação direta na recuperação do módulo. As informações geradas por estes mecanismos poderão ser úteis

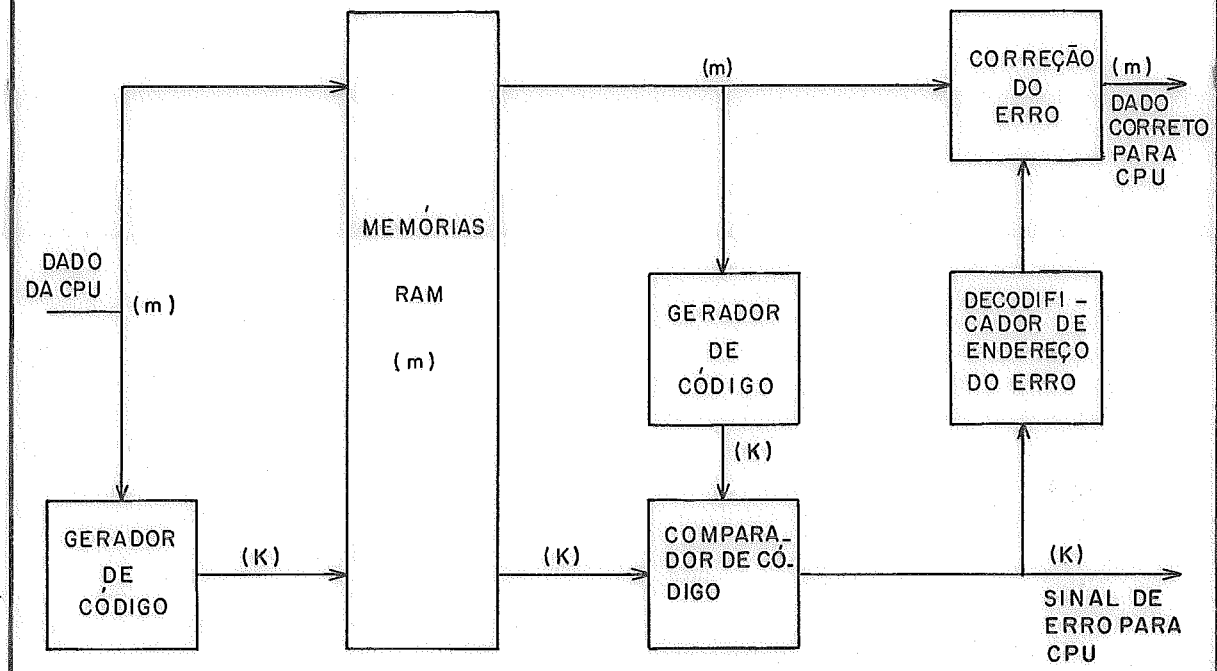


FIGURA (IV.8) – DIAGRAMA EM BLOCO DE UM CIRCUITO DE DETECÇÃO E CORREÇÃO DE ERRO NA MEMÓRIA

para outros mecanismos de detecção e recuperação de falhas.

i - Circuito de identificação do motivo de reinicialização do módulo - Este dispositivo consegue distingüir a origem da reinicialização ("watch -dog", paridade, proteção de memória, reset pela chave).

Como veremos adiante, estas informações serão transmitidas a um mecanismo externo de observação e serão úteis na análise posterior da eficiência das técnicas de recuperação e para estatísticas.

ii - Dispositivos para observação das fontes de alimentação.

Decidimos que não compensaria desenvolver mecanismos para observação de fontes de alimentação, isto porque o esquema proposto a seguir é muito simples e sendo o sistema distribuido, qualquer mecanismo de observação seria muito complexo.

Como veremos adiante, o esquema de alimentação adotado foi: um retificador e filtro, sendo o conjunto duplicado, são usados para alimentar um conjunto de operadores. Para cada operador usamos um regulador de voltagem para alimentá-lo.

O esquema de observação das fontes proposto foi:

a - Para os retificadores e filtros podemos usar medidores analógicos no painel para tensão e corrente;

b - Para os reguladores dos operadores é suficiente uma indicação luminosa no painel (LED) que indique o funcionamento do retificador.

O esquema da fonte e sua duplicação serão mostrados mais adiante na seção relativa a redundâncias.

iii - Circuitos para observação das interfaces de entrada e

saída do módulo.

Estes dispositivos determinam se o módulo está se comunicando através de suas interfaces de entrada e saída. Os sinais produzidos por estes circuitos poderão ser lidos pelo módulo e exteriorizados.

São dois os mecanismos propostos:

a - Comunicação com a VGI - como veremos na próxima seção o sistema é dotado de duas VGIs. Então, é importante verificar se as duas estão operando corretamente, se algum módulo não se comunica em uma delas,etc.

b - Comunicação com periférico - este dispositivo serve para identificação da falta de comunicação com o periférico e pode descobrir a existência de falhas ou no periférico ou na interface do módulo.

IV.4.2 - MECANISMO DE OBSERVAÇÃO DO SISTEMA

Este mecanismo permite uma otimização do desempenho, utilização e manutenção do sistema. Permite ainda uma avaliação real da disponibilidade e é útil para a realização de melhoramentos das técnicas de recuperação.

A função de observação do sistema não deve ter como meta apenas procedimentos de detecção de falha e recuperação do sistema. Aqui se pode implementar funções, tão complexas quanto se deseja, com o objetivo de se observar o estado operacional do sistema tais como: levantamento da configuração do sistema, registro de eventos ocorridos, estatísticas diversas, etc.

Como já foi dito, a observação do sistema pode ser vista como um sistema de supervisão e controle do próprio centro de supervisão e controle . Entretanto, as grandezas supervisionadas e exteriorizadas por este novo sistema de supervisão são de origem totalmente diferente daquelas do centro de supervisão e controle. As grandezas do sistema de

observação referem-se ao sistema computacional, as do centro referem-se ao sistema elétrico. Além disso, os dados serão manipulados por pessoas de formação totalmente diferente. Uns por técnicos de manutenção do sistema computacional, os outros pelos despachantes do sistema elétrico, respectivamente.

Para realização das funções de observação do sistema, criou-se mais um operador chamado Operador de Observação (OO). A criação de um operador específico justifica-se pelo fato de se desejar uma homogeneidade de funções, evitando que a supervisão do sistema seja feita por um operador, cuja função e estrutura de dados estejam intimamente ligados com a supervisão e controle do sistema elétrico. Por outro lado, a criação de um novo operador permite a implementação de novas funções de observação, sempre que for necessária, sem onerar ainda mais os outros operadores.

As funções realizadas pelo Operador de Observação são:

i - Levantamento da configuração do sistema.

Esta função consiste no levantamento do estado de todos os dispositivos do sistema. Esta configuração é apresentada na tela do console na forma de um diagrama. As seguintes informações são levantadas pelo OO:

- estado de todos os operadores;
- estado dos periféricos;
- estado da VGI;
- estado das remotas.
- etc.

ii - Estatística

A finalidade desta função é o levantamento de dados úteis na avaliação do desempenho do sistema e para estudo de melhoramentos que possam ser introduzidos.

- taxa de erros na VGI;

- taxa de erros nas comunicações externas;
- taxa de inicialização dos operadores;
- tempo de manutenção;
- taxa de falhas permanentes;
- taxa de falhas transientes;
- etc.

iii - Alarmes

A função alarme é responsável pelo registro da ocorrência de algum evento no sistema.

- motivo de inicialização de algum dispositivo;
- saída de funcionamento de algum dispositivo;
- entrada em funcionamento de algum dispositivo;
- substituição da unidade defeituosa pela sobressalente;
- resultado de auto-testes;
- início de carga de programa;
- fim de carga de programa;
- etc.

iv - Controle

Todo controle feito sobre o Centro de Supervisão deve ser realizado através do OO.

- colocar ou retirar de serviço um periférico;
- teste de impressora ou registrador gráfico;
- retirar ou colocar console em modo de treinamento;
- teste nas unidades sobressalentes;
- etc.

v - Integridade de Programas

Esta função observa se há no sistema algum operador que tenha ficado muito tempo sem pedir carga de programa. Caso exista, na primeira oportunidade o OO enviará a este operador um comando para que ele se carregue novamente.

Estas são as cinco funções previstas para o Operador de Observação. Entretanto, como foi visto anteriormente, caso durante a utilização do sistema venha surgir a necessidade de novas funções, a sua implementação não será onerosa para o sistema.

IV.4.3 MECANISMOS DE RECONFIGURAÇÃO

A reconfiguração do sistema consiste, basicamente, em suprir o sistema com unidades sobressalentes, visando a substituição daqueles que apresentam alguma falha permanente, garantindo a continuação da execução das funções consideradas vitais.

O conceito de funções vitais permite que o sistema não seja totalmente replicado, reduzindo extremamente o custo, já que somente aquelas unidades cuja função é indispensável ao funcionamento do sistema são replicadas. Como foi visto quando se definiu a disponibilidade do sistema, as partes vitais do sistema são:

- comunicação externa;
- comunicação interna;
- acompanhamento de todas as variáveis;
- impressão;
- fontes de alimentação.

Para cada uma das partes acima estudaremos as redundâncias propostas.

IV.4.3.1 - REDUNDÂNCIA PARA OS OPERADORES RESPONSÁVEIS PELAS COMUNICAÇÕES EXTERNAS

Como foi visto no capítulo anterior os operadores responsáveis pelas comunicações externas são o Operador de Master e os Operadores de Remotas, respectivamente.

Estudaremos as técnicas de redundância separadamente devido as peculiaridades de cada uma delas.

IV.4.3.2 - REDUNDÂNCIA DO OPERADOR DE MASTER

Devido à importância do Operador de Master no contexto do projeto, exige-se que ele seja duplicado, pois todos os dados do COR fluem por ele com destino ao COS. Assim, a proposta é que o conjunto (módulo básico, modem e canal) seja duplicado.

Entretanto, uma questão interessante que surgiu nesta fase do projeto, foi quanto à necessidade de se realizar o chaveamento cruzado entre o Operador de Master e o canal.

As figuras (IV.9) e (IV.10) mostram duas opções possíveis para a ligação com o COS.

Como mostraremos no próximo capítulo a estrutura da figura (IV.10) tem uma disponibilidade maior, devido ao circuito de chaveamento, que está em série com todo o sistema. Assim foi escolhido o segundo esquema de ligação com o COS.

IV.4.3.3 - REDUNDÂNCIA DOS OPERADORES DE REMOTAS

Devido ao grande número de operadores de remota não convém replicar todos eles, pois isso elevaria demasiadamente o custo do projeto. A melhor solução foi colocar um operador sobressalente para um certo grupo de Operadores de Remotas.

Levando-se em consideração alguns problemas tais como: fontes de alimentação, acomodação das placas nos "racks", cabeação e principalmente o problema de complexidade e expandibilidade do circuito de chaveamento, optamos por alocar um operador sobressalente para cada quatro Operadores de Remotas, para manter a flexibilidade e capacidade de expansão do sistema.

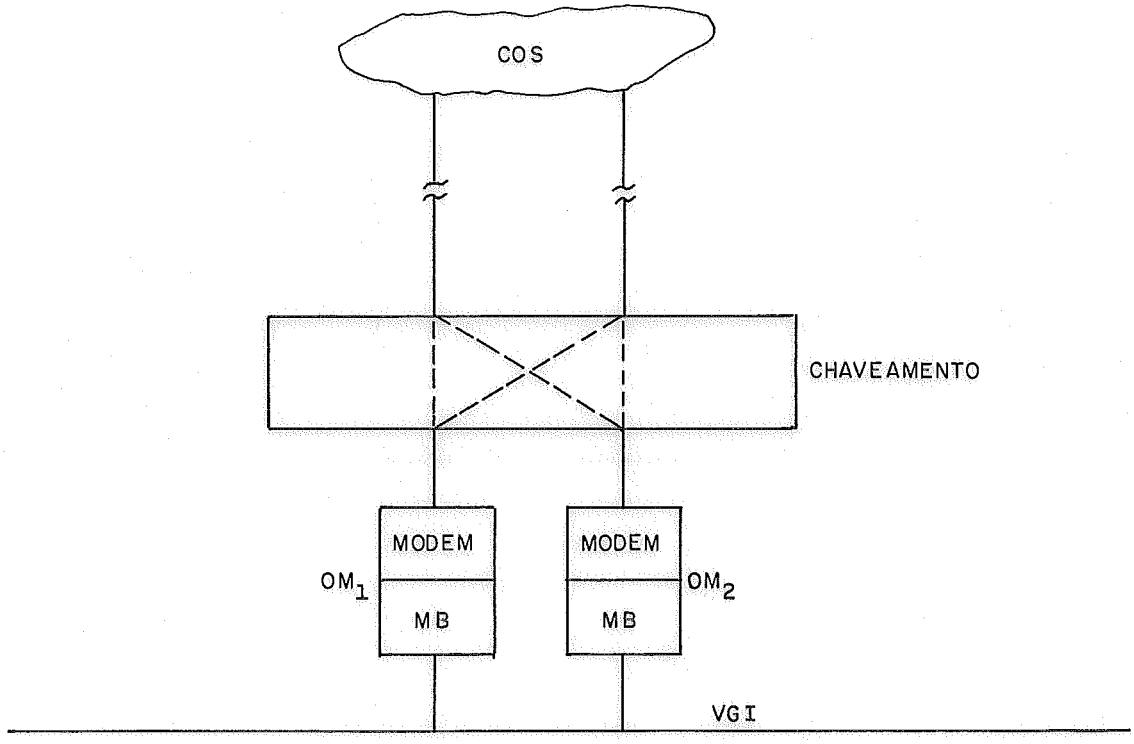


FIGURA (IV. 9) _ DUPLICAÇÃO DE OM COM CHAVEAMENTO A NÍVEL DE CANAL

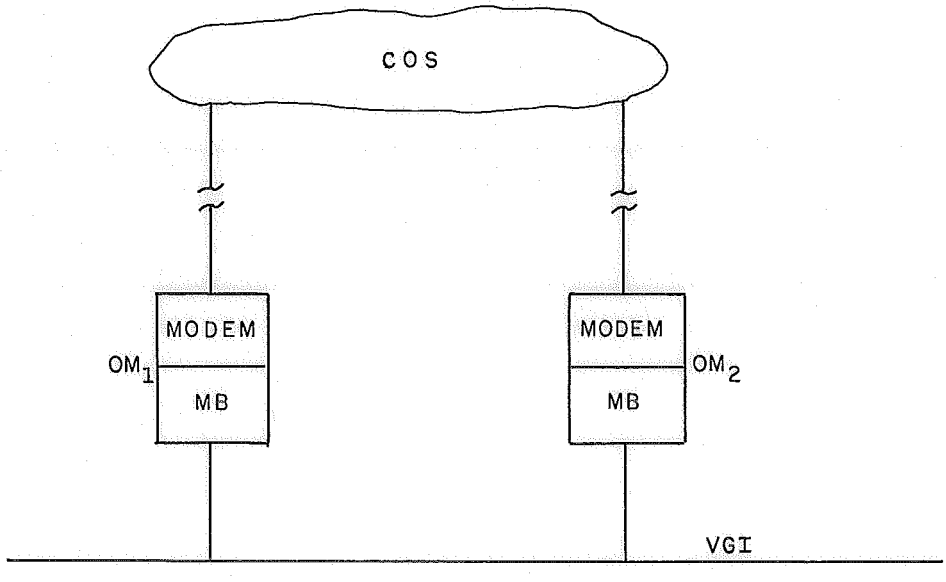


FIGURA (IV . 10): DUPLICAÇÃO DO OM SEM O CHAVEAMENTO

A figura (IV.11) mostra um exemplo de um grupamento de quatro Operadores de Remotas com o seu respectivo sobressalente. Neste esquema, o operador sobressalente fica supervisionando os quatro Operadores de Remotas do seu grupo. Caso uma falha retire um operador de funcionamento o operador sobressalente assumirá imediatamente o lugar daquele defeituoso.

Um aspecto muito importante a salientar, que será útil mais tarde durante a modelagem do sistema, é que o operador sobressalente é idêntico, em termos de "hardware", a um operador de remota. Assim, como ele permanece sempre alimentado, o operador sobressalente tem a mesma taxa de falhas de um Operador de Remota. Desta forma para se garantir que o esquema de chaveamento funcionará o operador sobressalente ficará constantemente sob supervisão do Operador de Observação. Além disto, periodicamente, desde que não esteja ocorrendo nenhum disturbio elétrico naquele instante, o operador sobressalente entrará no lugar de um operador de remota para testar seus circuitos de comunicação.

IV.4.3.4 - REDUNDÂNCIA DAS COMUNICAÇÕES INTERNAS (VGI)

Para garantir uma comunicação confiável a Via Geral de Interconexão (VGI) foi duplicada, garantindo a comunicação mesmo na presença de uma falha simples.

No caso específico da VGI, o meio físico para transmissão é apenas um fio. Por isto, poderia-se pensar que não há sentido em se duplicar um pedaço de fio. Entretanto, quando olhamos um pouco para dentro do módulo básico, podemos ver que não se trata apenas da duplicação de um fio.

A figura (IV.12) mostra a divisão de um módulo básico.

O acoplamento com o módulo consiste nos circuitos para transferência dos "bytes" que estão na memória para a via:

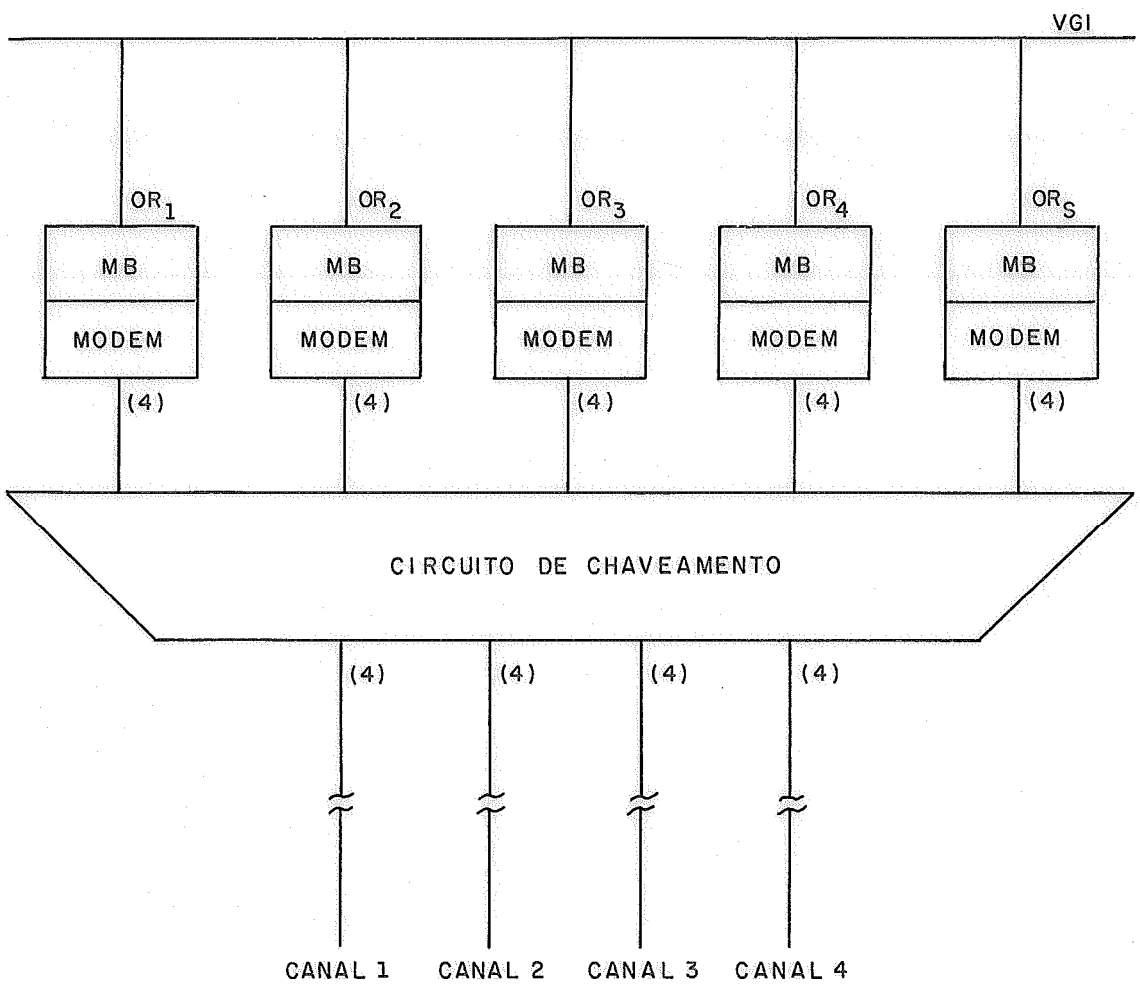


FIGURA (IV - 11) REDUNDÂNCIA DOS OPERADORES DE REMOTA

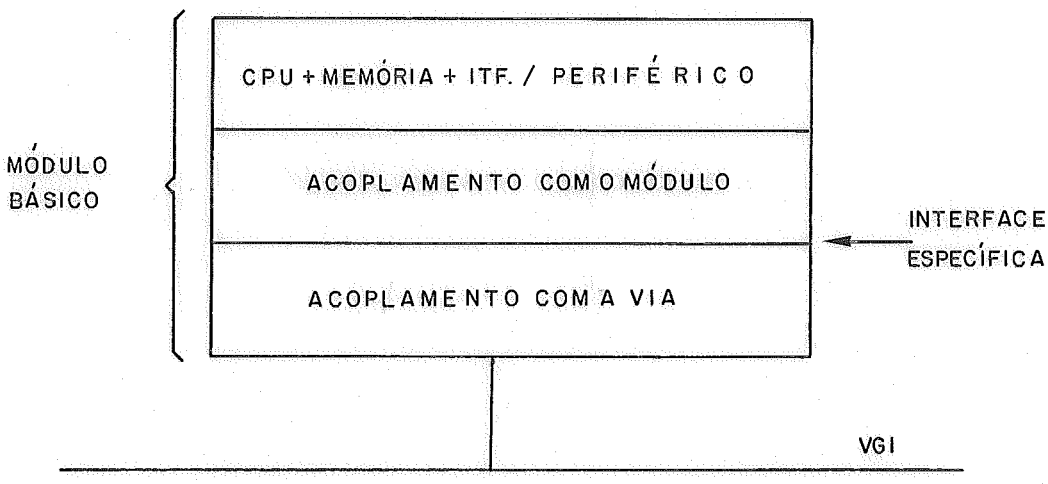


FIGURA (IV - 12) - LIGAÇÃO DE UM MÓDULO COM AVGI

controladores de interrupção, DMA e serializador. Consideramos que os circuitos de acoplamento com o módulo não pertencem a via, não havendo necessidade dele ser replicado.

O acoplador de via são todos os circuitos necessários para realização da conexão e acesso à via: circuitos excitadores, compatibilizadores de voltagem, isolamento, regeneração de relógio, detecção de colisão, codificadores, etc.

As figuras (IV.13), (IV.14) e (IV.15) apresentam as alternativas para duplicação da VGI.

As duas opções mostradas nas figuras (IV.14) e (IV.15) não foram implementadas, pois isto implicaria no uso de um acoplador de módulo com duas portas de entrada e saída, obrigando a duplicação de todos os "handlers" e rotinas do enlace físico. Isto tudo tornaria muito complexo o controle de acesso e comunicação na via.

Adotamos a solução mostrada na figura (IV.13), tendo sido duplicados apenas os circuitos de excitação de via ("drivers"), casadores de impedância, transformadores para isolamento, etc. Os circuitos responsáveis por regeneração do relógio, detecção de colisão, codificação, etc, que foram chamados de lógica na figura, não foram duplicados. Esta estratégia proporciona à VGI uma alta disponibilidade, pois os circuitos receptor/transmissor, por serem muito simples, garantem uma baixa taxa de falhas da VGI e mesmo no caso de falha de uma delas a outra, que é totalmente independente, garante o funcionamento do sistema.

Os circuitos receptor/transmissor foram projetados de tal modo a impedirem que uma falha no módulo se propague para VGI. Estes circuitos proporcionam um isolamento elétrico e lógico entre o módulo e a via.

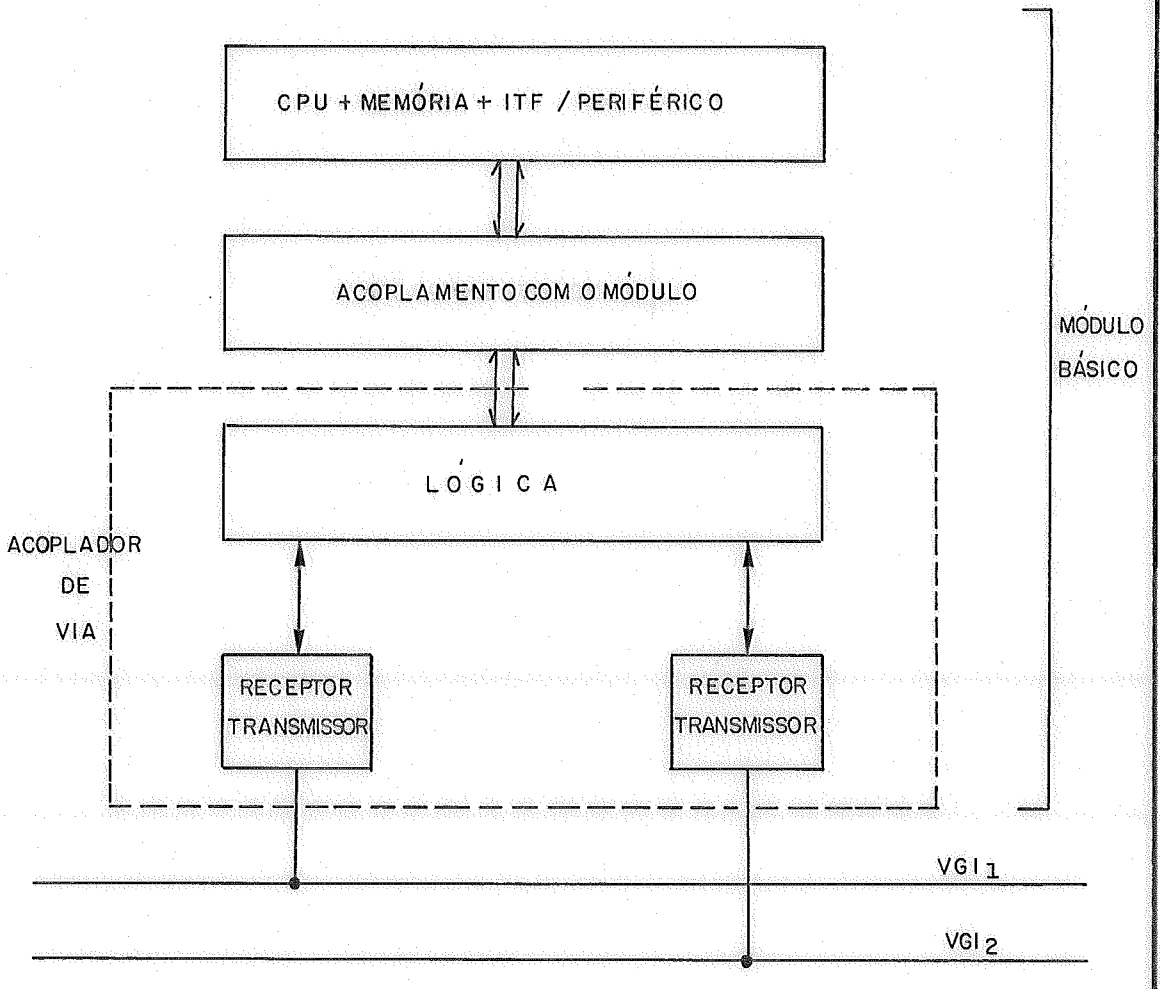


FIGURA (IV - 13) - REDUNDÂNCIA APENAS A NÍVEL DOS EXCITADORES DA VIA

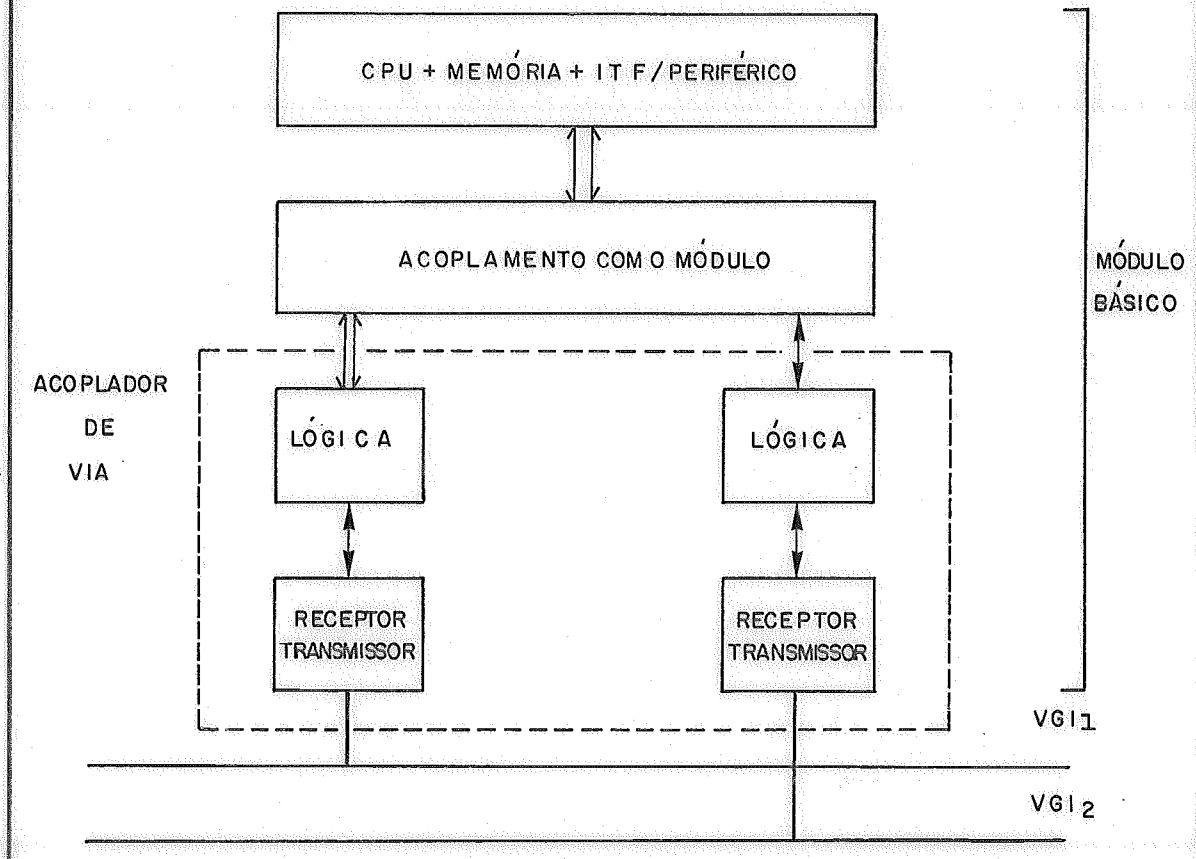


FIGURA (IV - 14) - REDUNDÂNCIA A NÍVEL DA LÓGICA

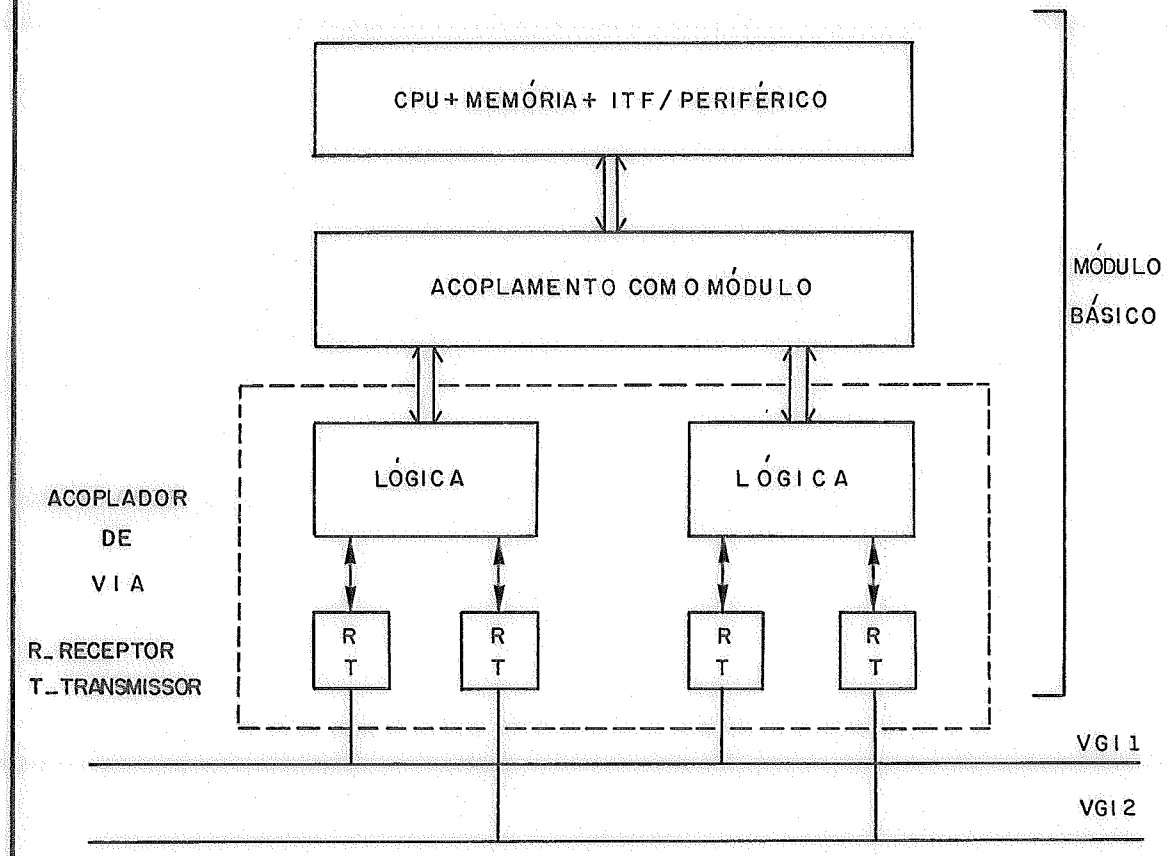


FIGURA (IV - 15) - REDUNDÂNCIA A NÍVEL DA LÓGICA COM OS EXCITADORES DUPLICADOS POR LÓGICA

IV.4.3.5 - REPLICAÇÃO DOS OPERADORES DE CONSOLE

Como vimos no capítulo anterior, o operador de console(OC) é o responsável pela maioria das funções de Interface Homem Máquina: acompanhamento das variáveis, geração de alarmes, tabelas, etc. Logo é fundamental que ele seja replicado.

Foi exigido que o projeto possuisse três postos de Interface Homem Máquina (teclado + dois CRT), para operação do sistema elétrico. Admite-se ainda a perda de até dois destes postos em caso de falha. Ou seja, é possível operar o sistema elétrico a partir de um posto apenas. Entretanto, esta condição é um caso crítico que não deve ocorrer freqüentemente, e caso ocorra não deve ser prolongada por muito tempo.

As figuras (IV.16) e (IV.17) mostram duas possibilidades de implementação do OC. A primeira apresenta apenas um operador controlando os três postos simultaneamente, no segundo caso foi associado um operador para cada posto, perfazendo um total de três OCs.

A primeira solução foi abandonada pois:

i - apresenta um elemento central, no caso o Operador de Console, que pode provocar a perda simultânea dos três postos de Interface Homem Máquina.

ii - O Operador de Console ficaria muito complexo.

A solução adotada foi a segunda, onde temos três postos de Interface Homem Máquina em funcionamento, cada um composto de um módulo básico, um teclado, dois CRT e um disco.

É importante ressaltar que este caso é diferente dos outros. Aqui não há redundância dinâmica (módulos sobressalentes). Os três OCs estão normalmente em funcionamento, sendo permitido que o sistema opere em modo degradado (com apenas um OC), por um curto espaço de tempo.

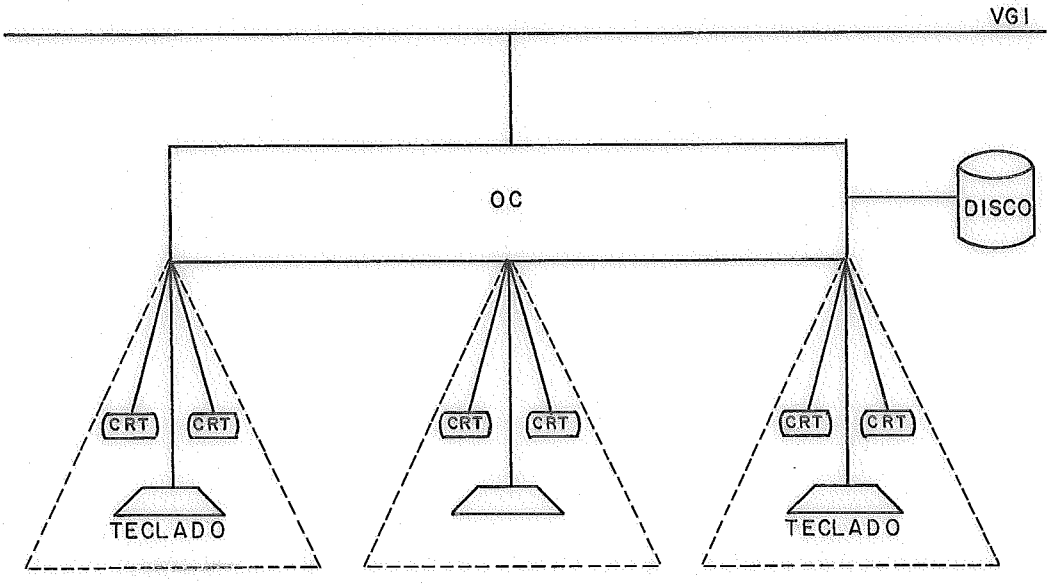


FIGURA (IV - 16) - ESTRUTURA COM UM OC TRÊS CONSOLES.

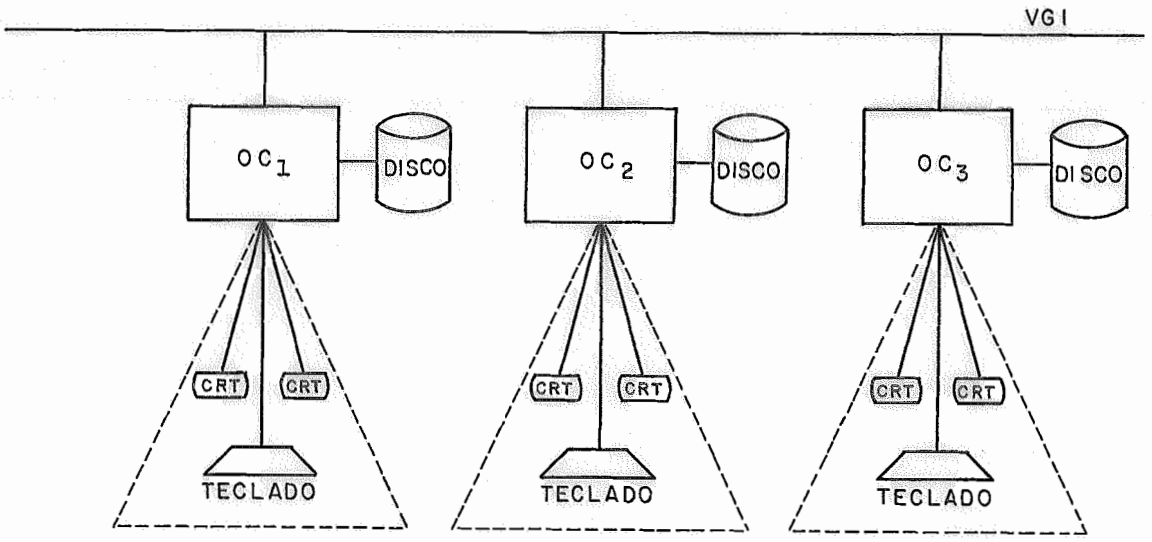


FIGURA (IV-17) - ESTRUTURA COM TRÊS OC_S

IV.4.3.6 - REPLICAÇÃO DO OPERADOR DE IMPRESSÃO (OI)

Um outro requisito para o Centro de Supervisão que deve ser atendido é a impressão de alarmes ou eventos e relatórios. Por problemas operacionais do COR a impressão de relatórios deve ficar separada da impressão de alames e eventos. Assim é importante que o operador de impressão tenha duas impressoras.

A duplicação do Operador de Impressão foi feita da seguinte maneira: Cada OI possui uma impressora para relatórios e outra para alarmes. Um deles fica operando e outro funciona como sobressalente. No caso de falha do OI em operação o outro assume imediatamente as funções de impressão. Se a falha for em uma das impressoras, o outro OI ativa apenas a impressora relativa aquela que parou.

A figura (IV.18) apresenta a estrutura replicada dos Operadores de Impressão.

IV.4.3.7 - REPLICAÇÃO DAS FONTES DE ALIMENTAÇÃO

A fonte de alimentação de um operador pode ser dividida em retificador e regulador. O retificador é o responsável pela transformação do sinal AC em DC e pela filtragem da tensão, o regulador serve para manter constante a tensão da fonte.

Por problemas de consumo, volume, montagem, etc., optamos por usar um regulador (circuito integrado) para cada operador e um retificador para um grupo de até cinco operadores. A figura (IV.19) mostra o esquema de uma fonte de alimentação sem redundância.

Quanto à introdução de redundância, optamos por duplicar apenas o retificador. Os reguladores não serão duplicados, pois consideramos que este pertence ao módulo. A falha do regulador implicará numa falha no operador respectivo.

Os retificadores foram dimensionados de modo que cada um deles possa alimentar todos os operadores. Em operação livre de

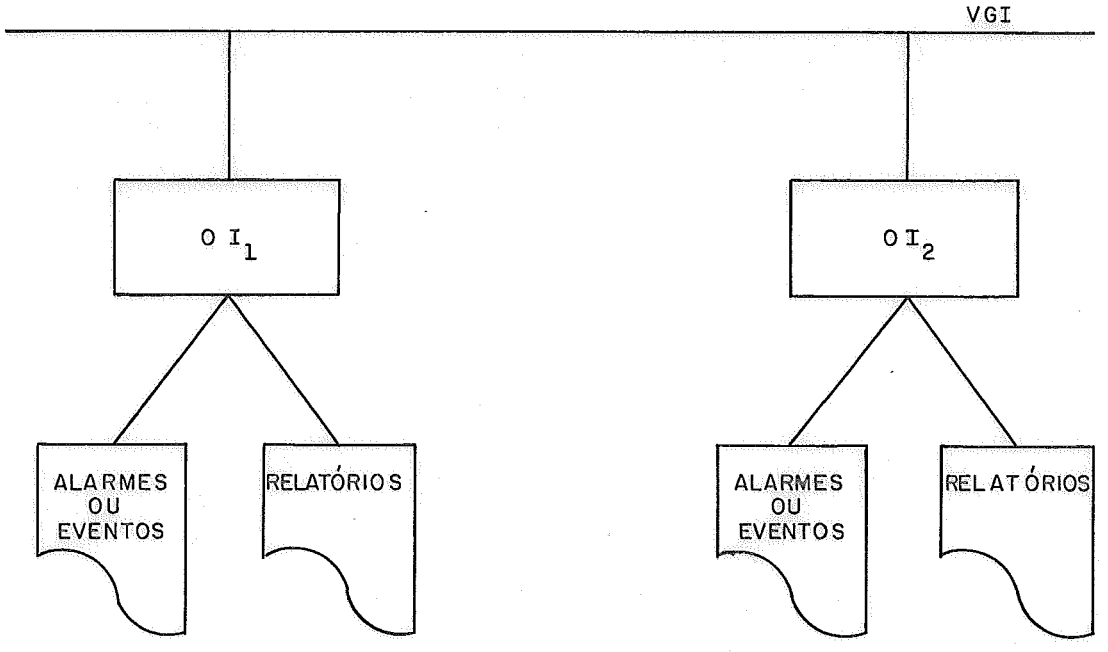


FIGURA (IV - 18) - ESTRUTURA REDUNDANTE DOS OI_1

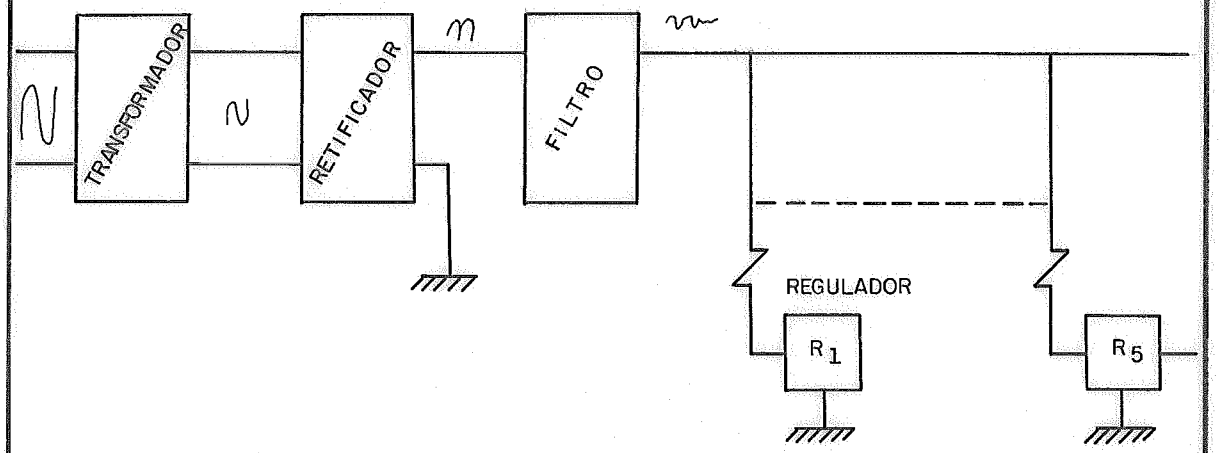


FIGURA (IV - 19)- FONTE SIMPLES

falhas, os dois retificadores dividem a carga entre si e em caso de falha de um, o outro continuará alimentando os operadores normalmente.

A figura (IV.20) apresenta o diagrama de uma fonte duplicada.

IV.4.4 - MECANISMOS DE RECUPERAÇÃO DO SISTEMA

IV.4.4.1 "WATCH DOG"

O "Watch dog" é uma técnica de "hardware" e "software" que tem como objetivo:

i - A detecção da perda de sequência do processamento de um módulo;

ii - Tentar recuperar o módulo através da reinicialização automática. Devemos observar que a recuperação do módulo só se efetivará caso a falha seja transiente. Para falhas permanentes, mesmo que o "watch dog" venha a atuar, nenhum efeito será observado.

Basicamente, esta técnica consiste num circuito específico (temporizador reengatilhável), que deve ser periodicamente resincronizado. Caso isto não ocorra o operador será reinicializado.

A figura (IV.21) mostra os diagramas de tempo de operação do "watch-dog". No primeiro caso o operador estava funcionando normalmente e em um dado instante parou de enviar o sincronismo. No segundo exemplo o operador passou a enviar o sincronismo numa frequência muito grande. Nos dois casos o operador deve ser inicializado.

Associado ao circuito descrito temos uma rotina de auto teste. Esta rotina é ativada periodicamente pelo sistema operacional, cabendo a ela enviar o pulso de sincronismo ao circuito do "watch dog". Entretanto, a rotina de auto teste só

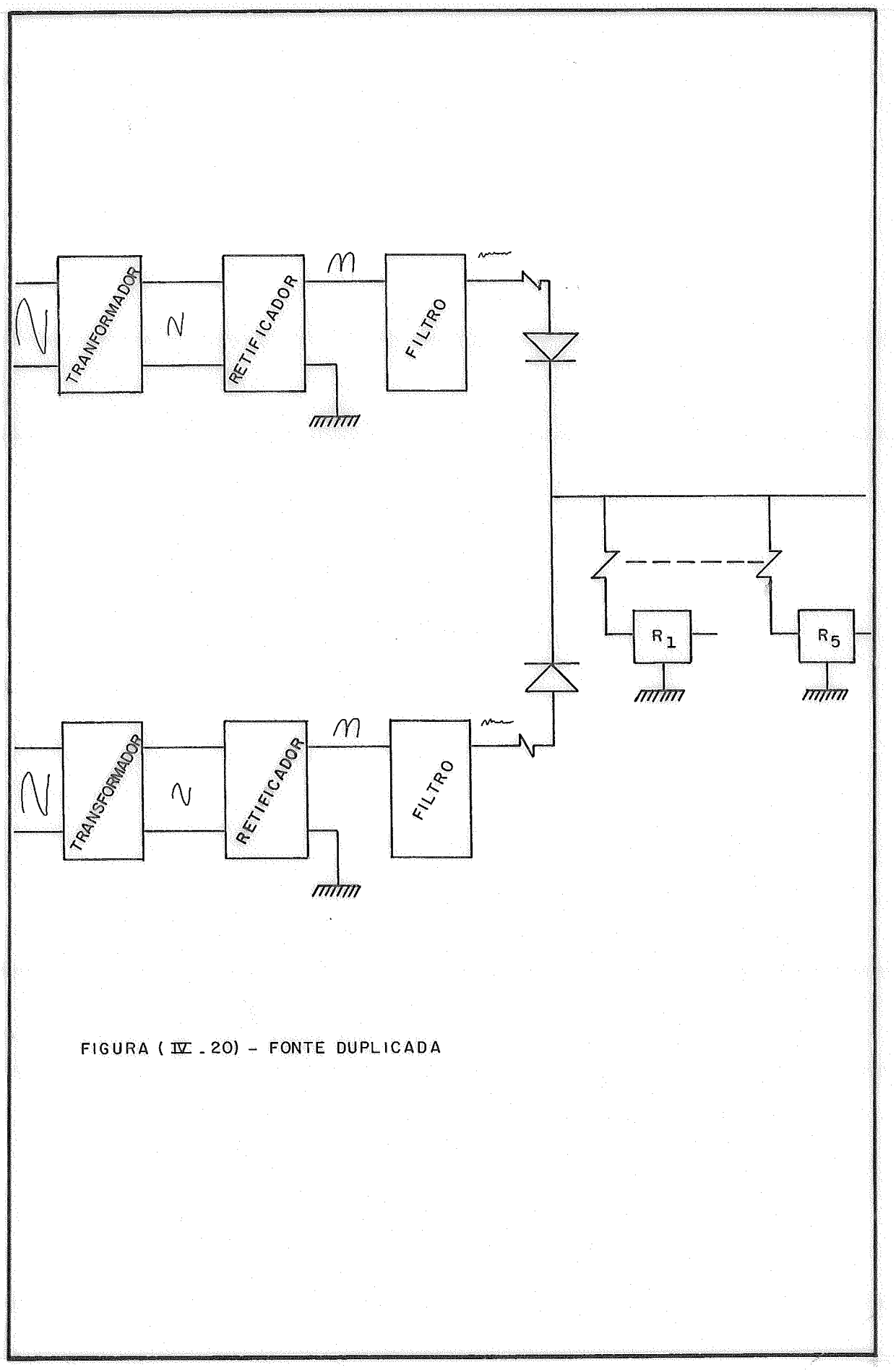


FIGURA (IV - 20) - FONTE DUPLICADA

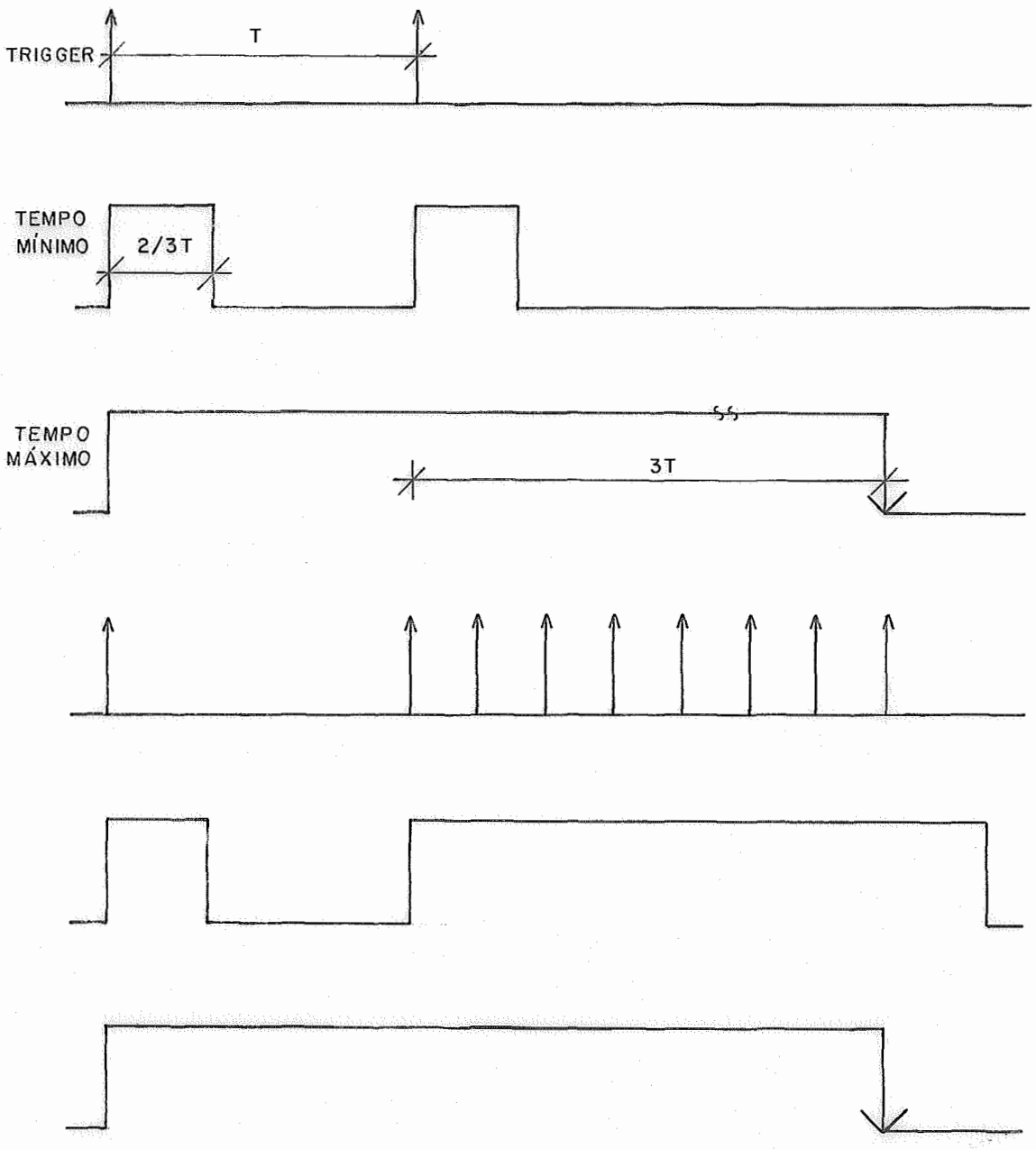


FIGURA (IV - 21) - DIAGRAMA DE TEMPO DO WATCH - DOG

enviará este pulso se o resultado dos testes realizados por ela evidenciar que o operador esteja executando corretamente suas funções. Ao se projetar um mecanismo de recuperação automática deve-se ter como metas o seguinte:

i - Minimizar o circuito do "watch dog" para que seja pequena a probabilidade de falha no próprio mecanismo, reduzindo assim a chamada interferência no processo de recuperação.

ii - Diminuir a influência do mau funcionamento do módulo no mecanismo de recuperação, ou seja, reduzir ao máximo os pontos de intercessão entre o módulo e o mecanismo de recuperação automática.

Devemos ter em mente que o "watch dog" não tem como objetivo a localização do defeito dentro do módulo, mas apenas detectar a ocorrência de uma falha. Sendo esta falha transiente ele deve tentar recuperar o módulo desta falha.

IV.4.4.2 ROTINA DE AUTO TESTE

Ao se projetar a rotina de auto testes a principal decisão está na escolha dos testes que devem ser realizados. Optamos por testes que não dependessem do próprio módulo.

i - Contabilização da ocorrência de eventos externos periódicos;

ii - Contabilização de ocorrência de eventos internos periódicos;

iii - Comparação do número de ocorrências contabilizadas anteriormente com determinados limites.

Assim, toda vez que ocorrer um evento que deva ser contabilizado, o contador correspondente àquele evento deve ser incrementado. Quando a rotina de auto teste for ativada, ela examinará estes contadores comparando-os com os respectivos limites. Caso todos os contadores estejam dentro dos seus

limites o circuito do "watch dog" é resincronizado. Caso contrário, a rotina de auto-teste não envia o sincronismo, permitindo que o módulo seja inicializado.

Para implementar esta função criamos a seguinte estrutura de dados apresentada na figura (IV.22). O vetor contador contém os contadores dos diversos eventos. CONTADOR-BARRA é o complemento de CONTADOR, somente para evitar a violação da estrutura. Os vetores MÁXIMO e MÍNIMO contém os limites dos contadores.

Com estes testes, pode-se ter uma idéia se não houve perda de sequência da execução do programa e se as interrupções estão chegando e sendo atendidas dentro da taxa esperada.

Alguns testes que podem ser realizados pela rotina de auto testes são:

i - Transmissão na VGI;

ii - Recepção pela VGI;

iii - Comunicação com o periférico;

iv - Execução periódica de rotinas;

v - Execução do processo de "back-ground";

IV.4.4.3 - ISOLAMENTO DO MÓDULO

Como foi visto anteriormente, o meio pelo qual um módulo pode propagar os efeitos de uma falha interna a ele é através de suas interfaces de entrada e saída. Assim, podem haver falhas que coloquem o módulo num estado tal que ele fique transmitindo constantemente ou para seu periférico ou para VGI, impedindo a reconfiguração do sistema ou até colocando o sistema em pane.

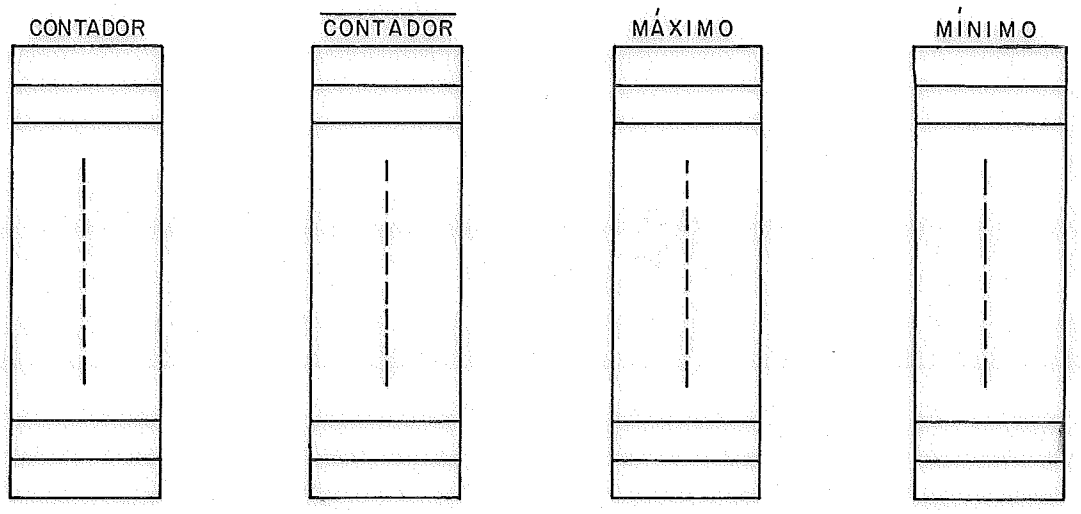


FIGURA (IV. 22) – ESTRUTURA DE DADOS DO WATCH-DOG

Esta técnica consiste em temporizar a transmissão de cada módulo. Caso ele insista em transmitir uma mensagem por um tempo muito grande, o módulo será desligado do sistema, sendo necessário a intervenção do ser humano para recolocá-lo no sistema.

CAPÍTULO V

MODELAGEM DO CENTRO DE SUPERVISÃO E CONTROLE

V.1 - INTRODUÇÃO

Vimos anteriormente que há duas maneiras de se avaliar a eficiência das técnicas de tolerância a falhas introduzidas em um sistema: experimental e analiticamente.

Devido à flexibilidade e ao baixo custo de se estimar analiticamente a disponibilidade (ou confiabilidade), o estudo de modelos tornou-se uma ferramenta importante e útil no projeto de sistemas tolerantes a falhas.

Neste capítulo descreveremos o modelo do Centro de Supervisão e Controle projetado pelo CEPEL. Usaremos como base o modelo desenvolvido por YING W.NG. e A.AVIZIENIS (1,21,22,23). Nestes trabalhos os autores sugerem como continuação para o seu trabalho utilizar o modelo na determinação da disponibilidade, já que eles deram ênfase ao cálculo da confiabilidade.

V.2 - DESCRIÇÃO DO MODELO

Primeiro apresentaremos o modelo usado para sistemas fechados, que não leva em consideração a manutenção. Depois mostraremos o modelo para sistemas com manutenção corretiva e finalmente introduziremos os parâmetros para falhas transientes, sendo, os dois primeiros, casos particulares do modelo geral.

V.2.1 - MODELO PARA SISTEMAS FECHADOS

Um sistema computacional tolerante a falhas pode ser dividido em um conjunto de subsistemas homogêneos, tais como

processador, memória, etc. No caso do Centro de Supervisão os subsistemas vitais que foram especificados são: subsistemas de comunicação com as remotas, comunicação com o nível hierárquico superior, console, impressão, VGI e fontes de alimentação.

Cada subsistema homogêneo consiste de um grupo de módulos idênticos, que podem ser ativos ou sobressalentes. Assume-se que para um sistema sobreviver, todos os subsistemas vitais devem sobreviver. Assim, a disponibilidade do sistema é o produto das disponibilidades dos subsistemas. Os parâmetros que são descritos abaixo dizem respeito apenas a um subsistema.

Um subsistema está perfeitamente caracterizado, em relação a falhas permanentes, com o seguinte conjunto de parâmetros (N,D,S, Ca, Cd,λ,μ,Y, CY), onde:

N - número inicial de módulos ativos;

D - número de degradações permitidas na configuração ativa (isto significa que o sistema pode perder até D de seus N módulos e ainda ser considerado em operação, ainda que degradada);

S - número de sobressalentes;

Ca - cobertura para detecção e recuperação de falhas em módulos ativos (isto é, a probabilidade de detecção e recuperação de falhas em módulos ativos sem paralisação do sistema);

Cd - cobertura para detecção e recuperação de falhas em módulos sobressalentes;

λ - taxa de falhas de um módulo ativo;

μ - taxa de falhas de um módulo sobressalente ($\lambda=\mu$ se o sobressalente estiver alimentado);

Y - seqüência de degradação permitida na configuração ativa;

configurações degradadas Y.

Os parâmetros (N,S, Ca, Cd,λ,μ) definem a capacidade de auto reparação do sistema.

A figura (V.1) mostra um modelo de macro estados para um sistema fechado (1). Neste diagrama está representada a evolução do sistema através de um subconjunto homogêneo composto de N módulos ativos e S sobressalentes, seguindo uma filosofia de chaveamento mostrada na figura (V.2).

No modelo, as falhas detectadas produzem transições desde o estado inicial (N,S,0) até o estado (N,0,0), que representa o sistema com suas redundâncias esgotadas, porém operando a plena capacidade. Falhas posteriores conduzirão o sistema a uma configuração degradada (caso degradações sejam permitidas). Uma falha não detectada em um módulo ativo leva o sistema a um estado de pane (P).

Entretanto, uma falha não detectada em um módulo sobressalente só colocará o sistema em pane quando este módulo for solicitado a entrar em operação. Este efeito é mostrado pelos estados $(\overline{N,S-1,0})$ até $(\overline{N,0,0})$. Os estados (N,i,0) e $(\overline{N,i,0})$ tem a mesma configuração ativa e o mesmo número de sobressalentes usados, entretanto, um sistema no estado $(\overline{N,i,0})$ perdeu sua capacidade de recuperação e degradação, pois existe um módulo sobressalente com uma falha não detectada.

Em algumas aplicações, depois de esgotados todas as redundâncias, admite-se que o sistema esteja operando corretamente, mesmo que mais falhas ocorram, desde que estas falhas sejam isoladas ou seus efeitos no sistema sejam mascarados e ainda permitam ao sistema uma capacidade operativa aceitável por certo tempo. O sistema passa então a operar numa configuração degradada, com um número menor de módulos ativos. Esta degradação é possível até uma configuração mínima, a partir da qual o sistema estará em pane. Esta capacidade de determinados sistemas é representada pelo vetor Y = (Y(1),Y(2),...,Y(D)), onde Y(i) é o número de módulos ativos

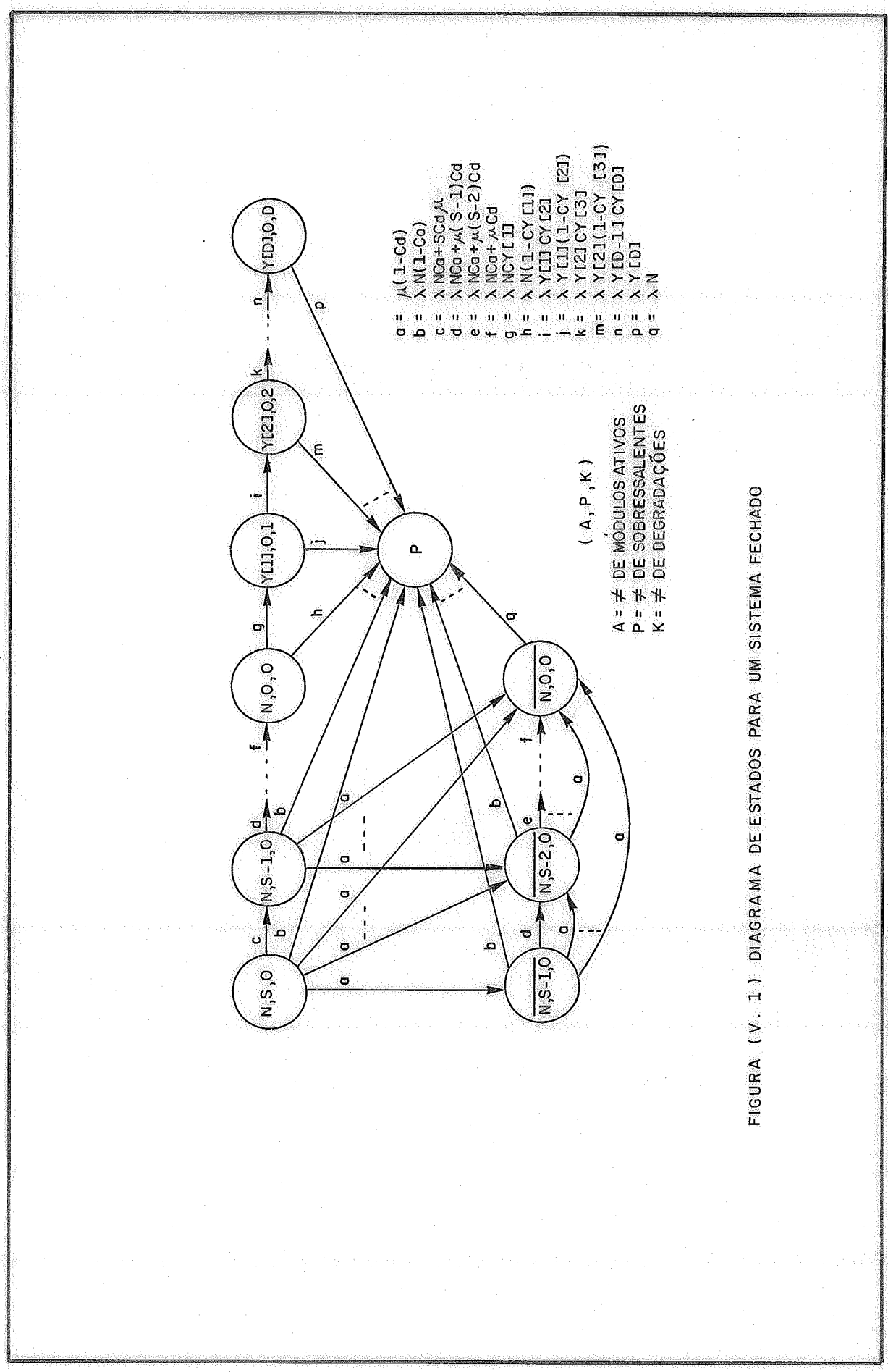


FIGURA (V. 1) DIAGRAMA DE ESTADOS PARA UM SISTEMA FECHADO

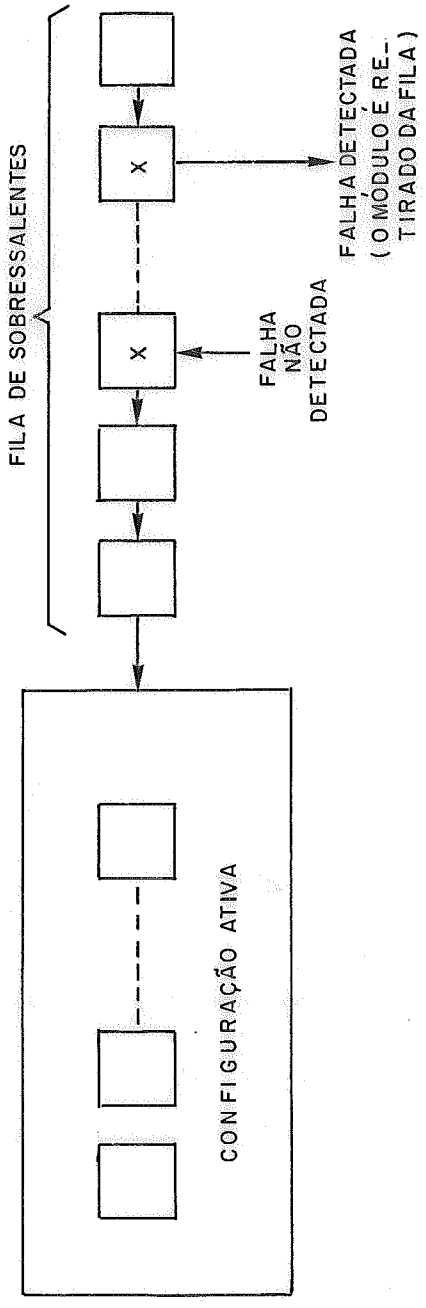


FIGURA (V. 2) _ FILOSOFIA DO CHAVEAMENTO DOS MÓDULOS SOBRESSALENTES

após a iésima degradação. Desde que o sistema esteja numa configuração degradada é possível que ele não tenha mais a mesma capacidade de detecção e recuperação de falhas. Isto é representado pelo vetor CY = (CY(1), CY(2),..., CY(D)), onde CY(i) é a cobertura associada à transição para o estado com a configuração Y(i) (por convenção CY(1) = Ca).

V.2.2 - MODELO PARA SISTEMAS COM MANUTENÇÃO

Existem muitas maneiras de se estender um modelo, desenvolvido para sistemas fechados, para ser usado em sistemas reparáveis, dependendo da maneira usada para modelar o processo de manutenção.

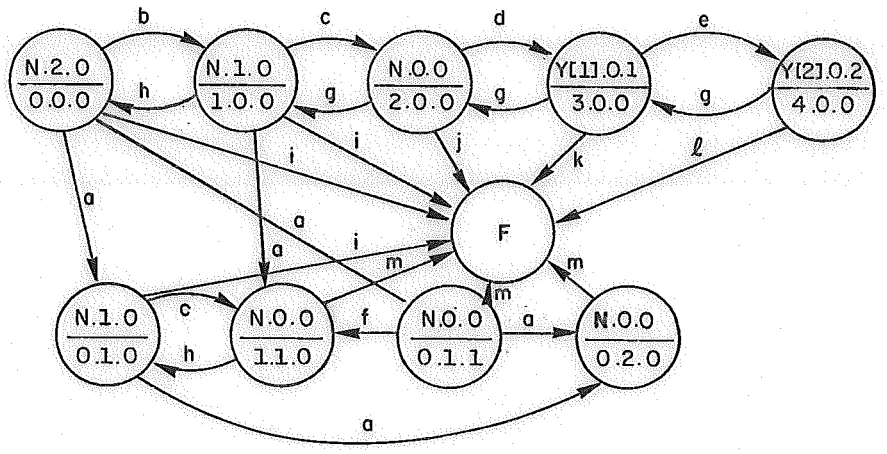
Neste modelo foi feita a suposição de que o processo de manutenção não tem memória, isto é, o tempo de manutenção é uma distribuição exponencial. Embora para algumas aplicações esta hipótese não seja muito precisa, ela é muito útil, pois permite o uso do mesmo modelo de Markov usado anteriormente nos sistemas fechados. Partindo-se desta hipótese, a manutenção do sistema fica caracterizada por uma taxa de manutenção constante.

No modelo desenvolvido foi também suposta uma capacidade múltipla e independente de se realizar a manutenção, cada uma com a mesma taxa de manutenção. Com estas hipóteses, um sistema tolerante a falhas reparável fica caracterizado com os mesmos parâmetros usados para sistemas fechados adicionando-se apenas mais dois parâmetros:

M = número de homens de manutenção (ou recursos de manutenção);

ψ = taxa de manutenção por homem de manutenção.

O conjunto completo de parâmetros para um sistema reparável é dado por (N,D,S, Ca, Cd,λ,μ,Y, CY,M,ψ). Este conjunto de parâmetro corresponde a um modelo de Markov mostrado na figura (V.3).



a = $(1-Cd)\mu$
b = $NCa\lambda + 2Cd\mu$
c = $NCa\lambda + Cd\mu$
d = $N\ CY[1]\lambda$
e = $Y[1]CY[2]\lambda$
f = $Cd\mu$
g = 2ψ
h = ψ
i = $N\lambda(1-Ca)$
j = $N\lambda(1-CY[1])$
K = $Y[1]\lambda(1-CY[2])$
l = $Y[2]\lambda$
m = $N\lambda$

$$\frac{A, P, K}{Q, R, B}$$

A ≠ DE MÓDULOS ATIVOS
P ≠ DE SOBRESSALENTES ACESSÍVEL
K ≠ DE DEGRADAÇOES
Q ≠ DE MÓDULOS EM MANUTENÇAO
R ≠ DE SOBRESSALENTES C/ FALHA SEM RECUPERAÇAO
B ≠ DE SOBRESSALENTES BONS BLOQUEADOS

FIGURA (V.3) – MODELO DE MARKOV PARA SISTEMAS REPARÁVEIS

(S = 2, D = 2, M = 2)

mostrado na figura (V.3).

Após a detecção de uma falha num módulo ativo, este é enviado para manutenção e um módulo sobressalente assume o lugar deste. Da mesma forma uma falha detectada em um módulo sobressalente provocará a ida deste para a manutenção, sendo este retirado da fila de sobressalentes. Para que uma falha em um módulo sobressalente seja detectada, este módulo deve ser testado periodicamente.

Depois que um módulo defeituoso for consertado ele voltará ao estado ativo, se o sistema estiver em modo degradado, ou então voltará à fila de sobressalentes.

Como num sistema fechado, uma falha não recuperada em um módulo ativo provoca, imediatamente, a pane do sistema. Entretanto, uma falha não detectada de um módulo sobressalente só provocará a pane do sistema quando este for solicitado.

A figura (V.3) mostra um modelo de Markov para um subsistema homogêneo com: N módulos ativos, dois sobressalentes, uma equipe de manutenção com dois homens, e uma capacidade de degradação de dois módulos. O esquema de chaveamento e manutenção é mostrado na figura (V.4)

No modelo da figura (V.3) se fizermos a taxa de manutenção igual a zero, podemos juntar os estados (N,0,0)/(1,0,0) ; (N,0,0)/(0,1,1) e (N,0,0)/(0,2,0) voltando ao modelo da figura (V.1).

V.2.3 - MODELO PARA FALHAS TRANSIENTES

É muito importante que um sistema tolerante a falhas tenha capacidade de se recuperar de falhas transientes. Devemos então modelar esta habilidade do sistema para avaliar a eficiência das técnicas empregadas e identificar maneiras de melhorar esta eficiência.

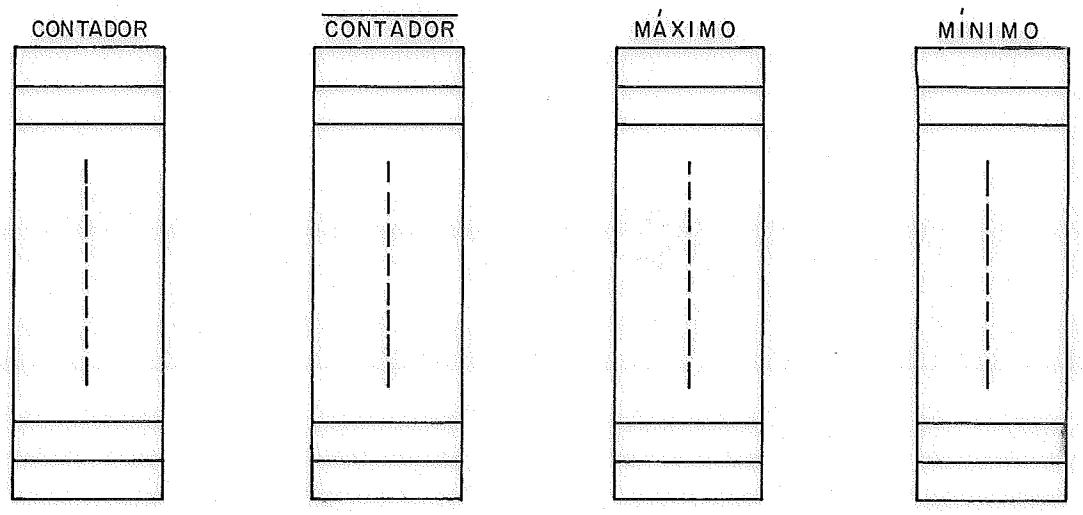


FIGURA (IV. 22) – ESTRUTURA DE DADOS DO WATCH-DOG

Vimos anteriormente que uma falha transiente é causada por um evento físico como uma interferência do meio, mau funcionamento temporário de um componente, etc. Uma falha transiente pode provocar danos imprevisíveis no sistema, entretanto, ela geralmente não causará danos permanentes de "hardware".

Uma falha transiente pode ser caracterizada por dois parâmetros: Taxa de chegada (T) e tempo médio de duração (D). Devido a falta de dados sobre a natureza estocástica das falhas transientes e o interesse de se usar um modelo de Markov único para falhas permanentes e transientes, foi assumido que a taxa de chegada e o tempo de duração de uma falha transiente constituem um processo de POISSON (T e D são constantes).

Para se ter uma tolerância a falhas transiente eficiente, usa-se uma combinação de várias técnicas, como já mencionadas no capítulo IV, estabelecendo-se uma estratégia de recuperação, composta de vários estágios. Cada estágio desta estratégia pode deixar de cumprir sua missão por uma série de razões, que resumiremos abaixo:

i - Transiente Persistente

Se uma falha transiente persiste por todo intervalo de tempo relativo a um estágio de recuperação, este estágio certamente não recuperará o sistema, cabendo ao próximo estágio tentar cumprir esta missão. Se a falha perdurar por todos os estágios esta falha será tratada como sendo permanente. A probabilidade de que estes eventos ocorram é descrita por T, D e também pelo tempo de duração do estágio i de recuperação T(i);

ii - Falha Catastrófica

Uma falha catastrófica é aquela que causa tantos danos ao sistema, que a recuperação deste se torna impossível.

Geralmente, uma falha catastrófica leva o sistema ao estado de pane antes mesmo que o primeiro estágio de recuperação seja executado. Chamaremos de r a probabilidade de que uma falha não seja catastrófica.

iii - Ineficiência

Embora uma falha não seja catastrófica, uma determinada técnica pode ser ineficiente contra ela. Isto é modelado pelo parâmetro chamado eficiência do estágio i (E(i)).

iv - Interferência

Os mecanismos de detecção e recuperação de falhas transientes também estão sujeitos a falhas. Estes fenômenos são modelados pela taxa de interferência, que é a taxa de falhas do "hardware" dos mecanismos de recuperação do sistema.

A recuperação de uma falha transiente pode ser modelada como um processo de fases múltiplas, conforme mostrado na figura (V.5). Existem três possíveis saídas para este processo: O sistema está em pane, a falha é tratada como uma falha permanente ou o sistema retorna ao seu processamento normal. Os três parâmetros definidos abaixo caracterizam a capacidade de tolerância a falhas transientes do sistema.

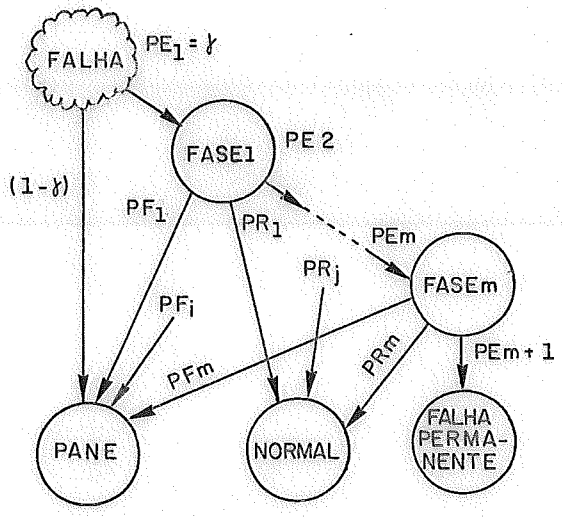
Ct = Cobertura transiente = prob(recuperação transiente ter sucesso/falha ocorreu).

Lt = fuga transiente = prob (falha ser tratada como permanente/falha ocorreu).

Ft = prob (sistema entrar em pane / falha ocorreu).

$$Ct = \sum_{1}^{m} PRi$$

$$Lt = PEm+1$$



FIGURA(V.5) - PROCESSO DE RECUPERAÇÃO DE FALHAS TRANSIENTES

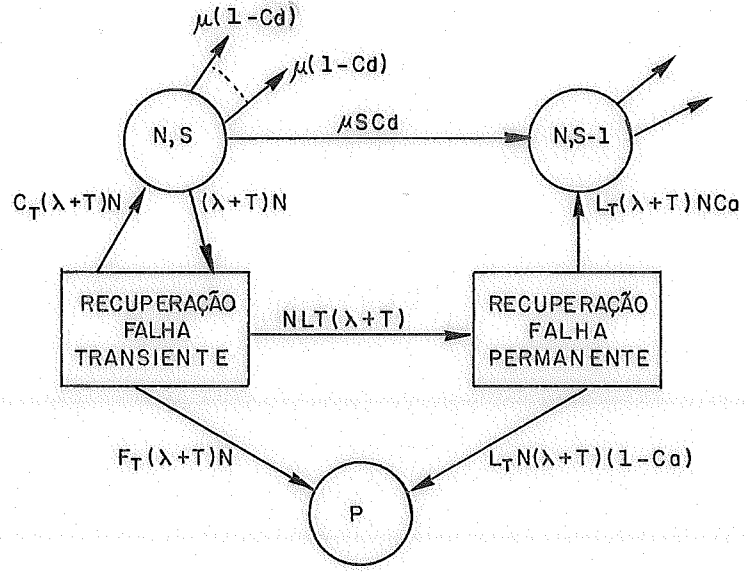
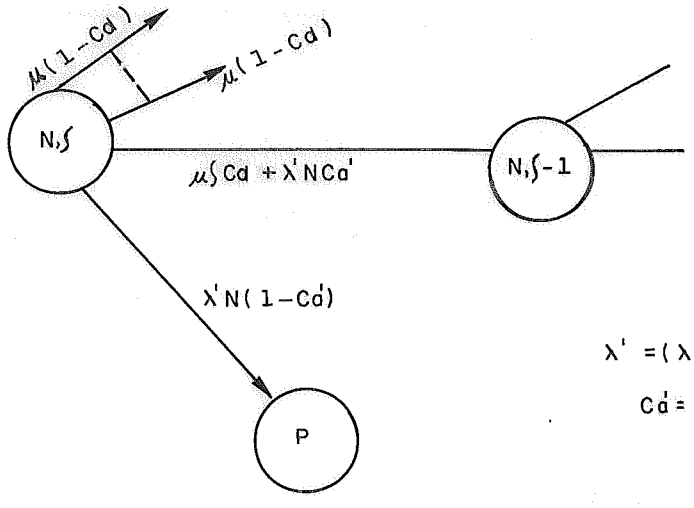


FIGURA (V.6) - MODELO DE MARKOV PARA RECUPERAÇÃO DE FALHAS TRANSIENTES



$$\lambda' = (\lambda + T)(F_T + L_T)$$

$$Cd' = \frac{Ca \; L_T}{F_T + L_T}$$

FIGURA (V - 7) - MODELO DE MARKOV EQUIVALENTE

$$Ft = (1 - r) + \sum_{1}^{m} PFi$$

PE = prob (sistema entrar na fase i de recuperação / falha ocorreu)

PRi = prob (sistema seja recuperado na fase i / falha ocorreu)

PFi = prob (sistema entre em pane na fase i / falha ocorreu)

onde:

PRi = prob (de entrar na fase i) x prob (da falha ser transiente) x prob (fase i ser eficiente) x prob (de não haver interferência nesta fase) x prob (não ocorrência de outra falha na fase i) x prob (duração da falha não se estender até a fase i).

PFi = prob (entrar na fase i) x prob (haver interferência).

PEi+1 = PEi - (PFi + PRi).

PE1 = r

PR1 = 0

PF1 = (1 - r)

A figura (V.6) mostra um modelo de Markov para recuperação de falhas transiente. A figura (V.7) mostra um modelo de Markov equivalente, incorporando a recuperação de falhas transiente ao modelo geral. Esta simplificação é possível pois o tempo dos processos de recuperação é várias ordens de grandezas menor que o tempo médio entre falhas. Assim, podemos considerar como sendo instantâneo o processo de recuperação de falha transiente.

Em qualquer instante de tempo, a probabilidade do sistema sair do estado (N,S) devido a uma falha em algum módulo ativo é:

$N\lambda'$ = taxa de falhas total dos módulos ativos - prob (retorno ao mesmo estado devido a uma recuperação com sucesso).

$$N.\lambda' = N.(\lambda + \gamma).(1 - Ct)$$

$$N.\lambda' = N.(\lambda + \gamma).(Lt + Ft)$$

$$\lambda' = (\lambda + \gamma)\ (Lt + Ft)$$

λ' = taxa de falhas transientes e permanentes.

A probabilidade de se entrar no estado (N, S-1) devido a uma falha em um módulo ativo é:

$$N.C'a\ .\ \lambda' = Ca.N.Lt.(\lambda + \gamma)$$

$$C'a = Ca.Lt/(Lt + Ft)$$

$C'a$ = corbetura de falhas transientes e permanentes

V.3 - MODELAGEM DO CENTRO DE SUPERVISÃO

Usaremos o modelo descrito na seção V.2 para calcular a disponibilidade do Centro de Supervisão, depois que foram introduzidas no sistema todas as técnicas de tolerância a falhas, descritas no capítulo IV.

Aplicaremos o modelo nos diversos subsistemas que foram considerados vitais para o funcionamento do Centro. Para cada um destes subsistemas calcularemos a disponibilidade, considerando inicialmente o índice de cobertura unitário. Em seguida calcularemos a disponibilidade total do sistema. Depois estudaremos a variação da disponibilidade com o índice de cobertura, determinando o índice de cobertura mínimo que o sistema deve ter. Finalizando, introduziremos as falhas transiente, usando os resultados obtidos no laboratório com o sistema de geração de falhas, descrito no capítulo VI.

V.3.1 - MODELAGEM COM ÍNDICE DE COBERTURA UNITÁRIO

V.3.1.1 - MODELO PARA O SUBSISTEMA DE COMUNICAÇÃO COM AS REMOTAS

O subsistema de comunicação com as remotas se caracteriza pelo grande número de Operadores de Remotas, o que inviabiliza a duplicação de todas os operadores. Assim, deve-se ter uma estratégia para se ter S módulos sobressalentes para N módulos ativos (S menor do que N).

Para obtenção do modelo fizemos as seguintes hipóteses:

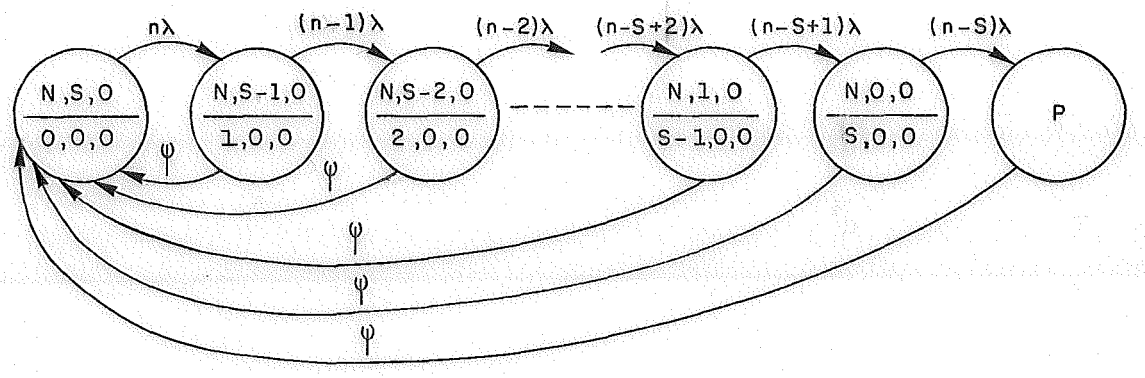
Ca = Cd = 1
$\lambda = \mu$
D = 0
M = 1
ψ = 100.000/Mh
Obs. Deste ponto em diante assumiremos que uma vez iniciada a manutenção o sistema voltará sempre ao estado ini ial.

A figura (V.8) apresenta o modelo de um subsistema de N módulos ativos e S sobressalentes. A disponibilidade deste subsistema é dada por:

$$A = 1 - \frac{\prod_{i=0}^{S} (n - i)\lambda}{\prod_{i=0}^{S} ((n - i)\lambda + \psi)} \qquad \text{fórmula (V.1)}$$

onde: n = N + S

No caso específico de FURNAS uma configuração típica para um COR seria de dezesseis Operadores de Remotas. Entretanto, para outras aplicações este número pode variar muito. Podemos ter casos em que seja necessário apenas alguns Operadores de Remotas. Em outros casos podem ser necessários vinte ou trinta



FIGURA(V.8) - MODELO PARA N MÓDULOS E $\int$ SOBRESSALENTES

N	DISPONIBILIDADE DE UMA CONFIGURAÇÃO (%)	DISPONIBILIDADE PARA 16 OPERADORES DE REMOTAS (%)	DISPONIBILIDADE COM CIRCUITO DE CHAVEAM. (%)
4	99,998	99,992	99,985
8	99,993	99,986	99,972
16	99,980	99,980	99,947

$S = 1$
$\lambda = 100\ f / 10^6 h$ (OR + MODEM)
$\psi = 10/10^6 h$ (TEMPO DE MANUTENÇÃO DE 10 HORAS)
$\lambda CH4 = 6{,}75 f / 10^6 h$
$\lambda CH8 = 13{,}5 f / 10^6 h$, $\lambda CH16 = 27 f / 10^6 h$

TABELA(V_1) _ DISPONIBILIDADE PARA ALGUMAS CONFIGURAÇÃO DE OPERADORES DE REMOTAS

Operadores de Remotas.

Por isto, optamos por uma estrutura modular colocando um operador sobressalente para cada grupo de quatro operadores de Remota. Assim, podemos ter uma estrutura de porte variável, para diversas aplicações. Além disto, esta escolha possibilita a realização de uma placa de chaveamento relativamente simples e de pequena taxa de falhas. A tabela (V.1) apresenta a disponibilidade de algumas configurações possíveis.

V.3.1.2 - MODELO PARA OS SUBSISTEMAS COM REDUNDÂNCIA DUPLA

Este modelo é usado para sistemas redundantes dinamicamente, sendo o sistema composto de um módulo ativo e outro sobressalente.

Este modelo é aplicável ao Operador de Master, Operador de Impressão, VGI e fontes de alimentacão.

A figura (V.9) apresenta o modelo de Markov para este tipo de sistema. A disponibilidade para um sistema deste tipo é dada pela fórmula (V.2).

$$A = 1 - \frac{2\lambda^2}{(2\lambda + \psi)(\lambda + \psi)} \qquad \text{fórmula (V.2)}$$

A partir dos seguintes valores, que foram obtidos no anexo, podemos obter as diversas disponibilidades:

TFom, TFoi = 50 f/Mh

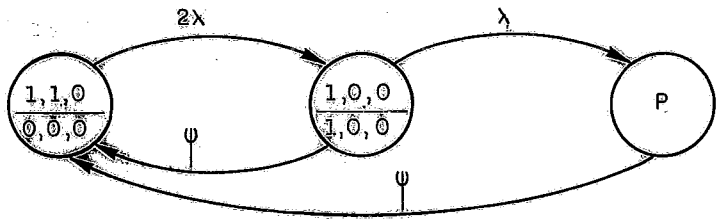


FIGURA (V - 9) - MODELO DE MARKOV PARA UM SISTEMA DUPLICADO

TFmodem = 100 f/Mh (modem 4800 bps)
TFimpressora = 100 f/Mh
TFvgi = 34,8 f/Mh (para uma configuração de 40 operadores)
TFfonte = 2 f/Mh

A tabela (V.2) mostra a disponibilidade para os vários subsistemas.

SUBSISTEMA	TAXA DE FALHAS/Mh	DISPONIBILIDADE
OM	150	1
OI	250	0,99999
VGI	34,8	1
FONTES	2	1

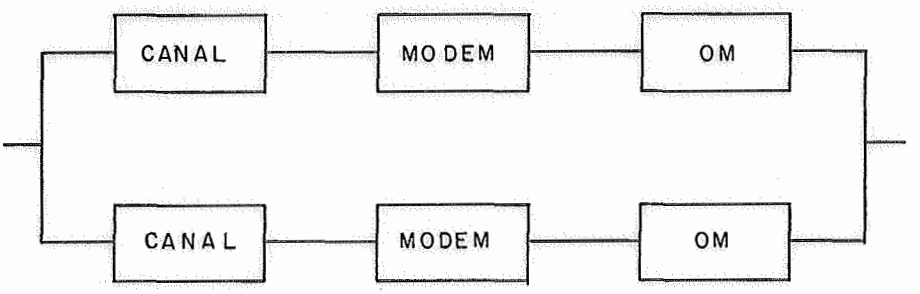
Tabela (V.2) - Disponibilidade dos Vários Subsistemas

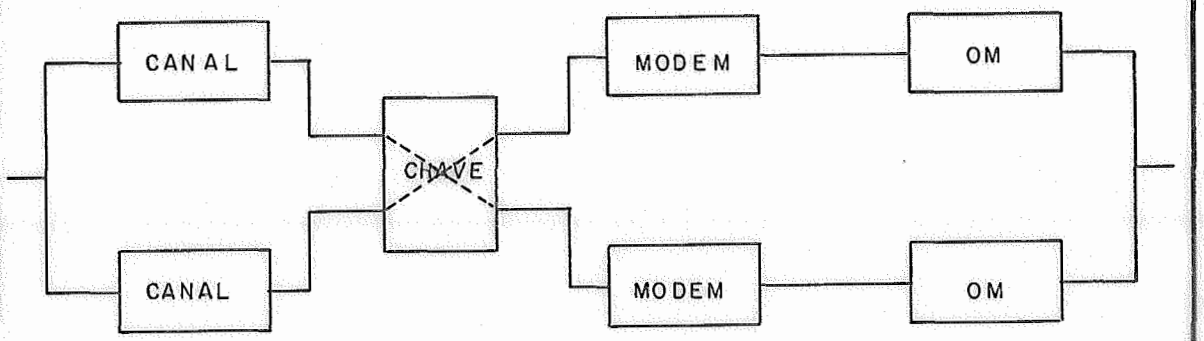
V.3.1.2.1 - DISPONIBILIDADE PARA AS DUAS OPÇÕES PARA LIGAÇÃO COR - COS

Como vimos anteriormente, haviam duas opções para ligação do COS ao COR.

A figura (V.10) mostra as duas opções. A primeira consiste na ligação do COS ao COR pelo sistema de comunicação (canal, Modem e OM), sendo o conjunto duplicado e sem chaveamento. Na segunda teríamos o chaveamento a nível de canal.

A disponibilidade do primeiro sistema é dada pela fórmula (V.2) onde:





FIGURA(V_10)_ OPÇÕES DE LIGAÇÃO C_oS __ C_oR

TF = TFcanal + TFmodem + TFom

No segundo caso a disponibilidade é o produto das disponibilidades das partes, pois estas estão em série.

A = Acanal.Achav.Aom+modem

onde: Acanal, Aom+modem - são dadas pela fórmula (V.2)

Obtivemos através de uma estatística que é mantida por FURNAS que a taxa de falhas de um canal é de 500 f/Mh.

TFchav = 5 f/Mh

Para o primeiro sistema obtivemos: TF = 650 f/Mh

A1 = 0,99992

Para o segundo sistema temos:

A2 = 0,99995 x 0,99995 x 1

A2 = 0,9999

Dos resultados obtidos concluimos que não houve melhoria na disponibilidade do sistema, assim não compensa se colocar um circuito para chaveamento à nível de canal. Por isto optamos pela primeira solução.

Como havíamos mencionado no capítulo II, os circuitos de chaveamento são uma das maiores dificuldades encontradas para realização de redundância dinâmica.

Obs. Observa-se que no primeiro caso é necessário apenas 1 homem para manuteção, enquanto no segundo são necessários

V.3.1.3 - MODELO PARA O OPERADOR DE CONSOLE

O subsistema de Console difere dos outros pois neste não há redundâncias. A figura (V.11) apresenta o modelo de Markov para os Operadores de Console.

A disponibilidade para o subsistema de Operadores de Console é:

$$A = 1 - \frac{6\lambda^3}{(3\lambda + \psi)(2\lambda + \psi)(\lambda + \psi)} \qquad \text{fórmula (V.3)}$$

onde:

$TF = TFoc + 2.TFcrt + TFdisco$

$TFoc = TFcpu + TFitf + TFmemória = 150\ f/Mh$

$TFoc, TFdisco = 100\ f/Mh$

$TF = 450\ f/Mh$

$\underline{A = 1}$

V.3.1.4 - DISPONIBILIDADE DO CENTRO DE SUPERVISÃO

A tabela (V.3) apresenta a disponibilidade do Centro de Supervisão.

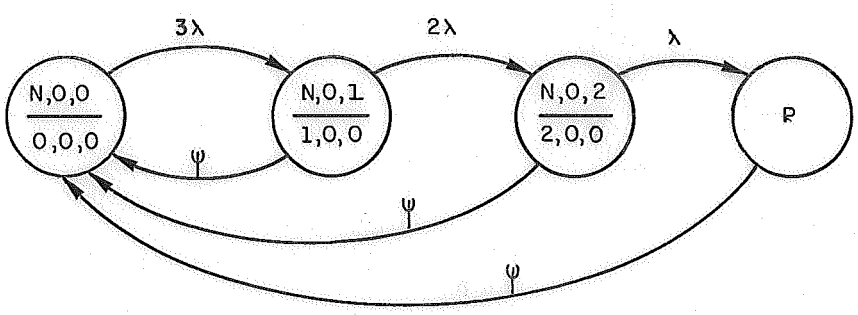


FIGURA (V - 11) - MODELO DE MARKOV PARA OS OPERADORES DE CONTROLE

SUBSISTEMA	DISPONIBILIDADE (%)
OM	100
OR	99,985
OC	100
OI	99,999
FONTES	100
VGI	100
TOTAL	99,984

Tabela (V.3) - DISPONIBILIDADE DO CENTRO DE SUPERVISÃO

Da tabela (V.3) o Centro de Supervisão tem uma disponibilidade maior que a especificada (99,8%), considerando como unitária (perfeita) a cobertura dos dispositivos de detecção e recuperação.

Na próxima seção estudaremos a variação da disponibilidade em relação à cobertura.

V.3.2 - MODELAGEM COM ÍNDICES DE COBERTURA MENOR QUE 1

Se considerarmos que as técnicas de detecção e recuperação de uma falha não são perfeitas, devemos então supor que a probabilidade dos sistemas recuperarem-se à falha é menor que um.

Para os subsistemas onde há redundância (comunicação com as remotas, comunicação com a estação central, impressão, VGI e fontes), o modelo da figura (V.12) mostra os possíveis estados

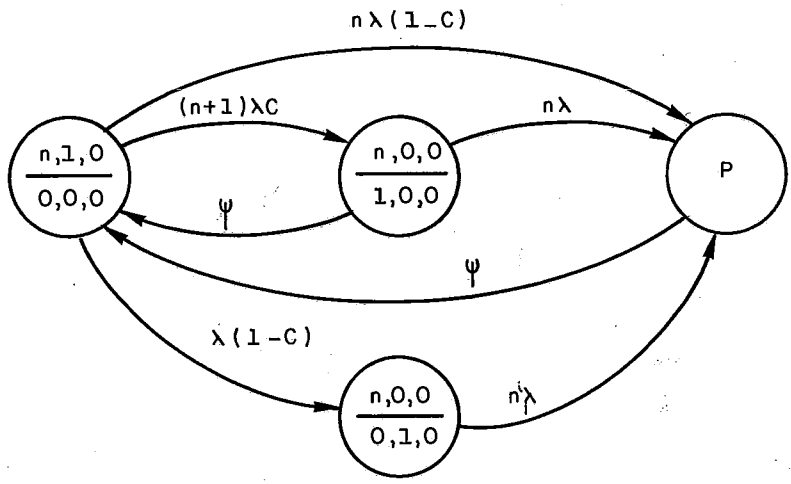


FIGURA (V – 12) – MODELO PARA UM SISTEMA COM n MÓDULOS E 1 SOBRESSALENTE (C ≠ 1)

estados de um sistema, considerando C diferente de um.

A disponibilidade de um sistema composto por N módulos ativos e um sobressalente é dada pela fórmula (V.4).

$$A = 1 \frac{n(n+1)(n\lambda + \psi - c\psi)\,\lambda}{(n(n+1)\lambda + n\psi + \bar{\psi}\,(1-c))(n\lambda + \psi)} \qquad \text{fórmula (V.4)}$$

No caso dos Operadores de Remotos temos n = 4, a disponibilidade é dada por:

$$A = 1 - \frac{80\lambda^2 + 20\lambda\psi - 20C\lambda\psi}{80\lambda^2 + 40\lambda\psi + 5\lambda^2 - C\lambda^2 - 4\lambda C\psi} \qquad \text{fórmula (V.5)}$$

Para o caso de n = 2 que se aplica aos outros subsistemas temos:

$$A = 1 - \frac{2(\lambda + \psi - C\psi)\,\lambda}{(2\lambda + \psi + \psi\,(1 - C)).(\lambda + \psi)} \qquad \text{fórmula (V.6)}$$

A figura (V.13) apresenta o modelo para os Operadores de Console. A disponibilidade do subsistema de Operadores de Console é dada pela fórmula (V.6) abaixo:

$$A = 1 - \frac{6\lambda + 6\lambda^2\psi - 6\lambda^2\psi C + 3\lambda\psi(\lambda + \psi) - 3\lambda C\psi(\lambda + \psi)}{(3\lambda + \psi)\,(2\lambda + \psi)\,(\lambda + \psi)}$$

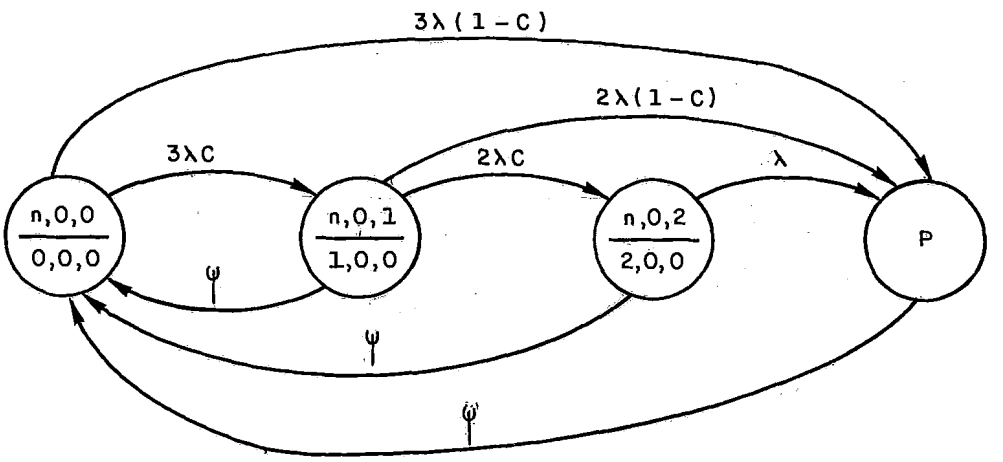


FIGURA (V - 13) - MODELO PARA OS OPERADORES DE CONTROLE

Aplicando as fórmulas (V.6) e (V.7) obtemos a tabela (V.4) que contém os diversos valores da disponibilidade para vários valores de C.

	0	0,92	0,94	0,96	0,98	1
OR	.9841	.9983	.9987	.9991	.9995	.9998
OM	.9985	.9998	.9998	.9999	.9999	1
OI	.9975	.9996	.9997	.9998	.9999	1
VGI	1	1	1	1	1	1
FONTES	1	1	1	1	1	1
OC	.9867	.9989	.9992	.9995	.9997	1
TOTAL	.9671	.9966	.9974	.9982	.9990	.9998

Tabela (V.4) - Variação da Disponibilidade em função da Cobertura

Analisando os resultados da tabela (V.4) e sempre tendo por objetivo a obtenção de um índice de disponibilidade total para o sistema superior a 0,998, concluimos que as coberturas oferecidas pelos dispositivos de detecção e recuperação de falhas devem ser tal que este índice seja alcançado. Isto se verifica, por exemplo, no caso em que todas as coberturas estejam em torno de 96%.

V.3.3 - MODELO PARA SISTEMA INTRODUZINDO AS FALHAS TRANSIENTES

Devemos agora obter os novos índices de cobertura e as novas taxas de falhas introduzindo a ocorrência de falhas transientes.

A figura (V.14) aplica o modelo da figura (V.5) para a aplicação considerada. Deve-se observar que apenas uma fase de recuperação foi implementada na atual versão (estado RECUP. AUTOMAT. na figura).

r - Probabilidade da falha não ser catastrófica;

E - Eficiência dos testes;

Ar - Probabilidade dos circuitos de recuperação estarem funcionando;

k - Probabilidade da falha ser transiente.

Ar = 0,99993 (TFr = 7f/10 Mh)

Avgi = 0,9999998

Aoc = 0,9999995

k = TFtransiente / (TFpermanente + TF transiente)

Da figura (V.14) podemos tirar ainda:

Ct = k.r.E.Ar.Avgi.Aoc fórmula (V.8)

Lt = r.Avgi.Aoc.(1 - k.E.Ar) fórmula (V.9)

Ft = r.(1 - Avgi.Aoc) fórmula (V.10)

Neste ponto, podemos ver o grande número de parâmetros que precisam ser estimados para dar prosseguimento ao estudo. Alguns destes parâmetros podem ser estimados (Ar,Avgi e Aoc),

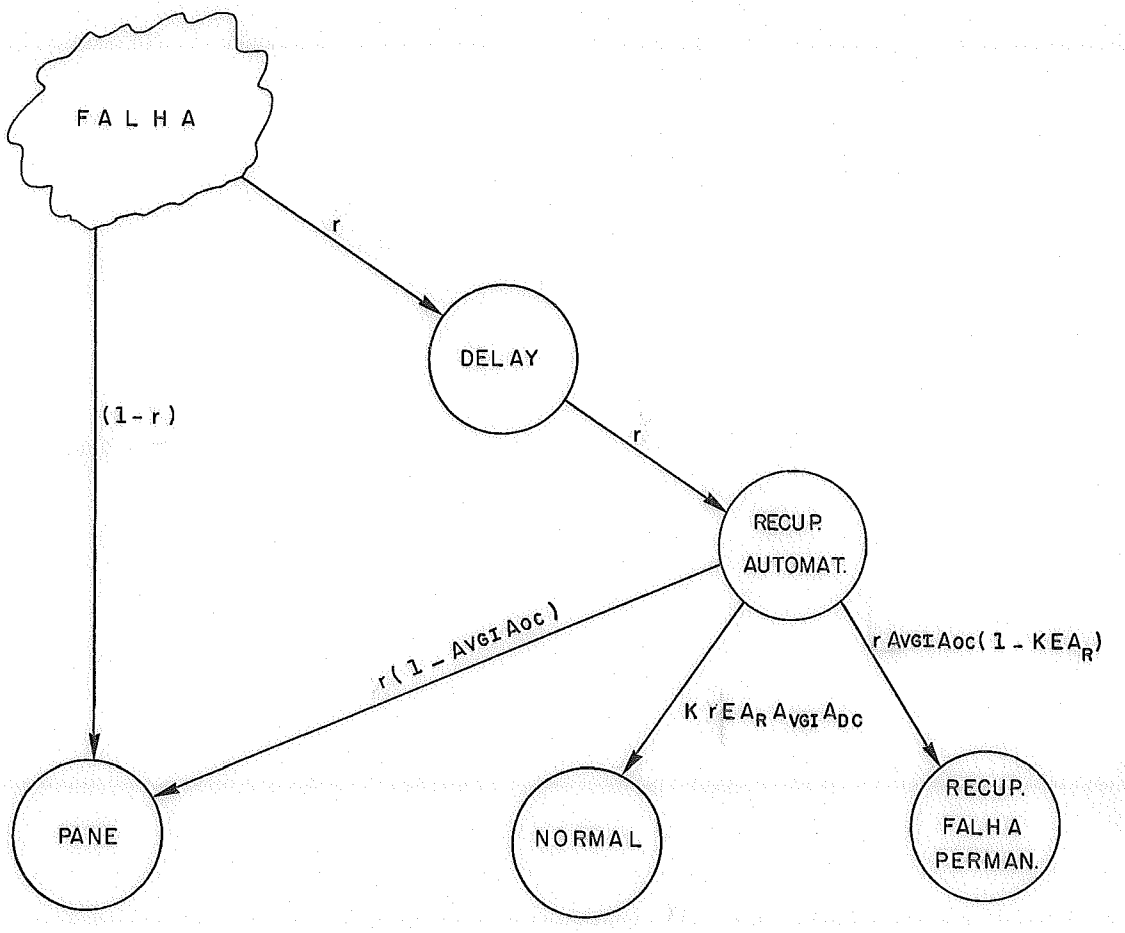


FIGURA (V - 14) - ESTADOS DE UM MÓDULO DURANTE A RECUPERAÇÃO DE UMA FALHA

outros serão atribuídos valores aproximados (k,r) e finalmente o valor de E será medido.

Com o objetivo de se medir o valor de E desenvolvemos um sistema capaz de gerar falhas sobre um módulo, que esteja em testes, contabilizando o número de falhas recuperadas automaticamente. No capítulo VI descrevemos com mais detalhes este sistema. Para dar prosseguimento adiantaremos que o valor medido de E foi de 0,9999.

Quanto ao valor de k (probabilidade da falha ser transiente), como não dispomos de nenhuma informação a respeito, e nem de como estimar o valor da taxa de falhas transientes, faremos a seguinte hipótese: k = 0,90

Um importante conceito em computadores tolerantes a falhas é aquele chamado "HARDCORE", que significa a parte mínima do sistema que precisa ficar livre de falhas para que o sistema seja capaz de se recuperar. O "HARDCORE" pode ser constituido por "hardware" e nestes caso existem métodos de proteção deste. Mas existe ainda o "HARDCORE" no "SOFTWARE" do sistema, constituido por programas e informações de controles vitais ao sistemas. Em sistemas ultra confiáveis deve-se manter cópias, protegidas destas informações (1).

Existem muitas outras razões que podem tornar uma falha catastrófica. Entretanto, devemos observar que este conceito de falha catastrófica é muito importante para sistemas onde se exige altíssima confiabilidade e onde não se tem acesso manual. No nosso caso, como vimos no capítulo II, o sistema pode ser controlado manualmente. Assim, no caso dos mecanismos de recuperação falharem, o operador humano poderá reinicializar o módulo, ou mesmo ordenar uma substituição do módulo defeituoso. Finalmente, a única informação que é vital para o sistema está no disco do Operador de Console, e este é triplicado.

Por tudo que foi exposto anteriormente adotamos o valor de r como sendo a unidade (r = 1).

Entrando com os valores destes parâmetros nas fórmulas (V.8), (V.9) e (V.10) obtemos:

$Ct = 0,90$

$Lt = 0,10$

$Ft = 0,0000007$

Usando o modelo da figura (V.7) temos:

$\lambda' = (\lambda + \gamma).(Ft + Lt)$ fórmula V.11)

$C' = C.Lt / (Ft + Lt)$ fórmula V.12)

$\lambda' = 1,1.\lambda$

$C' \cong C$

A tabela (V.6) mostra a variação da disponibilidade com a cobertura, levando-se em conta agora a taxa de falhas transientes. Vemos das equações (V.11) e (V.12) que houve um aumento na taxa de falhas dos módulos de 10% e que os índices de cobertura praticamente não se alteraram.

V.4 - ANÁLISE DOS RESULTADOS

Analisando os resultados obtidos no capítulo V, vemos que:

i - Considerando apenas as falhas permanentes e:

- Considerando os mecanismos de detecção e recuperação perfeitos (cobertura = 1), o sistema tem uma disponibilidade de 99,984%, acima da especificada (99,8%);

	0	0,92	0,94	0,96	0,98	1
OR	.9825	.9981	.9986	.9990	.9994	.9998
OM	.9984	.9998	.9998	.9999	.9999	.1
OI	.9973	.9996	.9997	.9998	.9999	1
VGI	1	1	1	1	1	1
FONTES	1	1	1	1	1	1
OC	.9854	.9988	.9991	.9994	.9997	1
TOTAL	.9639	.9963	.9972	.9980	.9989	.9998

TABELA (V.5) - Variação da disponibilidade do Sistema com a Cobertura levando-se em conta as falhas transientes.

- Fazendo-se uma análise um pouco mais rigorosa, introduzindo-se nos modelos o conceito de Cobertura, descobrimos que é necessário uma cobertura de no mínimo 96%, para se obter a disponibilidade especificada;

ii - Considerando também as falhas transientes:

- Os mecanismos de detecção e recuperação de falhas transientes mostraram-se eficientes e o valor da cobertura (96%), exigida anteriormente, praticamente não se alterou, ou seja, a disponibilidade do sistema continua basicamente dependendo da cobertura de falhas permanentes.

Pode-se agora, de posse destes resultados, decidir onde investir caso se deseje aperfeiçoar ainda mais o sistema.

CAPÍTULO VI

AVALIAÇÃO DA EFICIÊNCIA DAS TÉCNICAS DE DETECÇÃO E RECUPERAÇÃO AS FALHAS TRANSIENTE

VI.1 - INTRODUÇÃO

A modelagem da disponibilidade do sistema levando-se em conta as falhas transiente é função da eficiência das técnicas de recuperação, conforme foi mostrado no capítulo V . Por isto, torna-se necessária a obtenção de valores que meçam esta eficiência.

Os métodos de avaliação dos índices de eficiência das técnicas podem ser classificados em duas categorias:

i - TEÓRICOS

Consistem na obtenção do modelo analítico do sistema através de sua função de transferência T e no mapeamento do vetor de entrada E. Desta forma obtém-se o vetor de saída S = T.E. A falha transiente F pode ser encarada como uma superposição à entrada E. Desta forma tem-se que: S = T.(E + F).

Este método apresenta o inconveniente de ser difícil obter tanto as funções T como o vetor de entrada E para um sistema que apresenta um grande número de variáveis e estados. Para a obtenção de T deve-se poder modelar o comportamento interno dos diversos circuitos, principalmente em condições de funcionamento anormal. Estes dados dos dispositivos utilizados, circuitos comerciais, não estão disponíveis nos manuais, onde o comportamento dos CIs são apresentados de forma macroscópica.

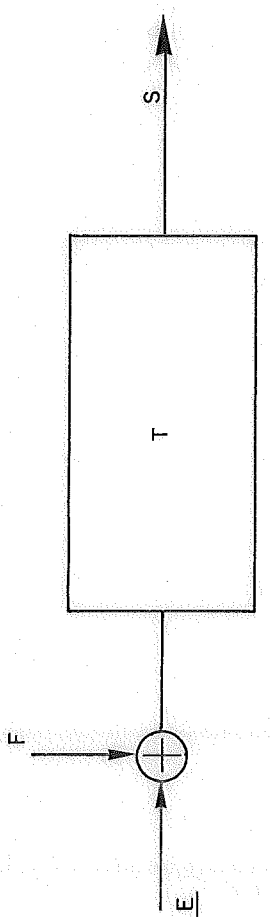


FIGURA (VI - 1) - SISTEMA SUJEITO A UMA FALHA

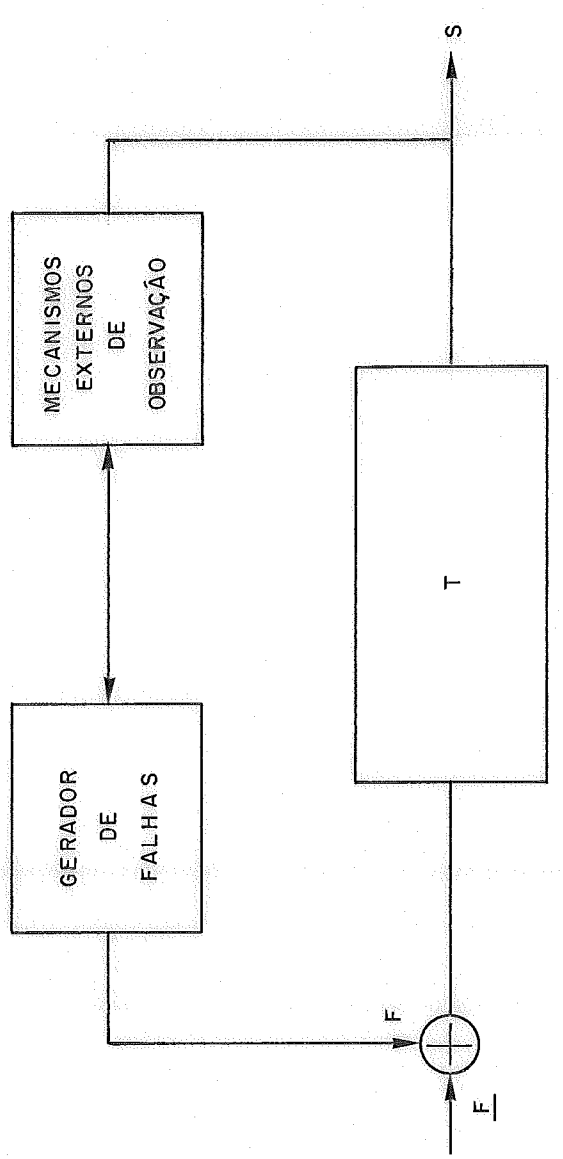


FIGURA (VI - 2) - MECANISMO DE AVALIAÇÃO DAS TÉCNICAS DE DETECÇÃO E RECUPERAÇÃO DE FALHAS

ii - PRÁTICOS

Consiste em se usar o próprio sistema (hardware + software) como elemento básico à avaliação. Desta forma, não é necessária a obtenção da função de transferência T. O elemento básico deve ser acrescido de duas partes:

a) mecanismos de aceleração das taxas de falhas transiente: Estes têm como responsabilidade gerar a função F de forma programada (frequência e energia de cada falha);

b) mecanismos externos de observação: estes deverão ser responsáveis pela análise do vetor S, contabilizando os diferentes estados de funcionamento, produzindo estatísticas e índices de eficiência de cada uma das técnicas de recuperação introduzidas.

Este método permite a observação rápida, porém, não é completo, dado que não se pode garantir que o sistema foi exercitado em todos os seus estados. Deve-se notar que o método teórico de avaliação apresenta esta restrição, porém, em um grau menor, pois pode-se exercitar mais seletivamente o sistema. Deve-se notar porém, que os resultados obtidos podem servir como uma primeira aproximação ao valor real (análise absoluta) e como índice de comparação entre as diversas técnicas (análise relativa).

VI.2 - DESCRIÇÃO DO SISTEMA DE AVALIAÇÃO DA EFICIÊNCIA DAS TÉCNICAS DE RECUPERAÇÃO

O método empregado neste trabalho para a avaliação de eficiência das técnicas de recuperação foi o prático. O sistema de testes implementado pode ser dividido em duas partes:

i - Módulo Padrão:

Apresenta uma configuração típica de um operador do

sistema. Neste módulo são acrescentados mecanismos de recuperação de forma independente. Desta forma, pode-se analisar as técnicas, primeiro isoladamente, depois conjuntamente;

ii - Módulo de Geração de Falhas e de Observação de Funcionamento

Possui uma configuração de "hardware" semelhante ao do módulo, acrescido de um gerador de falha, pois este "hardware" se encontrava disponível. Este foi construído de tal forma a funcionar em paralelo com qualquer componente (circuito integrado), sem interferir no funcionamento deste, até que seja gerada uma falha em um de seus pinos. A forma de onda da falha é uma onda quadrada, segundo a figura (VI.3)

Este perfil de falha foi escolhido por ser fácil a sua geração (circuitos necessários à implementação). O tempo de permanência foi arbitrado de tal forma a interferir na situação de funcionamento normal do sinal do pino do integrado, no qual se quer gerar a falha.

O método de observação consiste, apenas, em analisar um ponto do conjunto de saídas possíveis. O ponto de verificação escolhido foi a comunicação correta na via geral de interconexão (VGI). O módulo em análise será considerado em funcionamento se for capaz de se comunicar na VGI, enviando um "status" de funcionamento normal.

A figura (VI.4) apresenta o esquema usado para realização dos testes para avaliação da eficiência das técnicas de recuperação de falhas transientes.

VI.2.1 - DESCRIÇÃO DOS TESTES IMPLEMENTADOS

O teste implementado consiste em gerar em cada pino de todos os integrados do módulo submetido ao teste, uma forma de onda igual a da figura (VI.3).

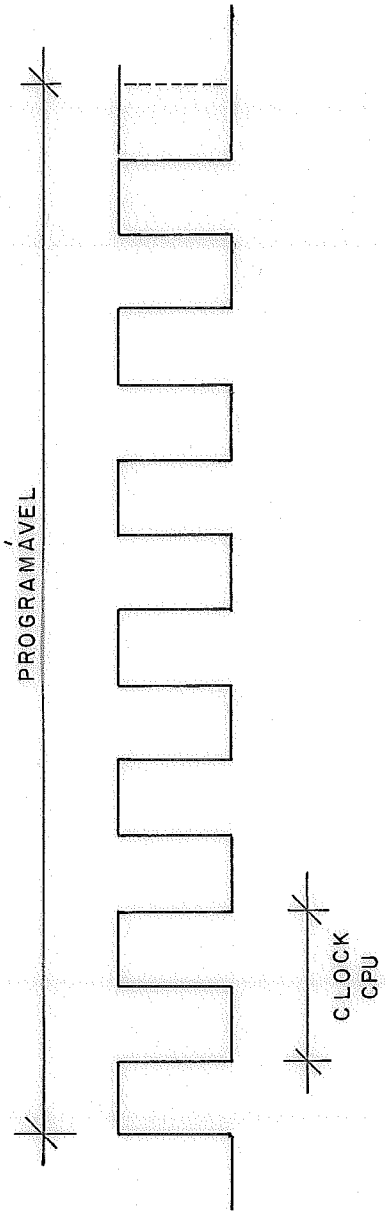


FIGURA (VI-3) – FORMA DE ONDA DO RUÍDO GERADO

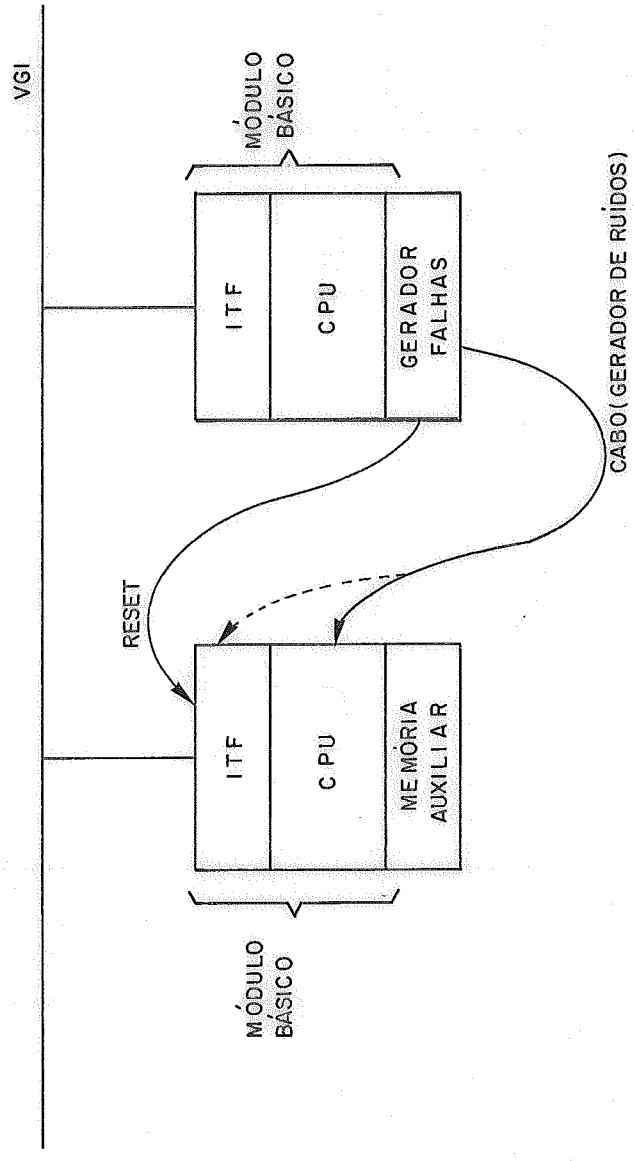


FIGURA (VI_4) - ESQUEMA DE TESTE

Após gerar o ruído, o módulo gerador de falhas espera um determinado tempo para que os mecanismos de recuperação reconduzam o módulo sob teste ao seu estado normal de funcionamento. Caso não se efetive a recuperação deste módulo, o próprio gerador de falhas enviará um pulso de "reset" ao módulo em teste.

A verificação do estado de funcionamento do módulo em teste é feita através da VGI. Foi estabelecido um protocolo de comunicação entre os dois módulos.

A título de estatística, o módulo gerador de falhas realiza as seguintes estatísticas:

i - número de falhas geradas;
ii - número de falhas não recuperadas;
iii - número de falhas não recuperadas por pino de cada inte rado.

Com o objetivo de acelerar o processo de recuperação do módulo sob teste, optamos por manter o programa do operador em uma memória auxiliar do tipo EPROM. Assim, durante a inicialização do módulo, o programa é transferido da memória auxiliar para a memória principal. Em condições normais o programa deverá ser carregado do OC através da VGI. Este processo gasta aproximadamente 20 segundos, enquanto o primeiro cerca de 1 segundo.

VI.3 - RESULTADOS DOS TESTES

Foram realizados uma série de testes para avaliação das técnicas propostas. Como exemplo, usamos um operador de Master e obtivemos os seguintes resultados:

i - sem técnicas de detecção e recuperação, observamos que 40% das falhas geradas, produziram efetivamente uma falha no módulo em teste;

ii - com os mecanismos implantados a cobertura obtidas foi de 9 ,98%.

Como vimos no Capítulo V, a cobertura transiente de um módulo é obtida pela fórmula (V.8).

$$Ct = k.r.E.Ar.Avgi.Aoc$$

No caso do teste tivemos:

k = 1 (todas as falhas geradas foram transientes)
r = 1 (não se observou falhas catastróficas).

Para este teste não foi usado a VGI e o OC para carga de programas, tendo sido usada uma memória do tipo EPROM para armazenar o programa do Operador de Master. Assim a fórmula (V.8) torna-se:

$$Ct = E.Ar.Am \qquad (VI.1)$$

onde:

Ar = 0,99993 (disponibilidade dos circuitos de recuperação automática).

Am = disponibilidade da memória auxiliar.

A memória auxiliar é composta de 3 EPROM (2732), um decodificador (8205) e um TTL (7400). A disponibilidade destes circuitos é 0,99994 (5,7 f/Mh).

Substituindo estes valores e o resultado dos testes na fórmula (VI.1) temos a eficiência das técnicas propostas.

E = 0,9999

VI.4 CONCLUSÃO

Dos resultados obtidos podemos concluir que a eficiência das técnicas que foram implementadas superaram em muito as expectativas, recuperando quase totalmente as falhas geradas.

CAPÍTULO VII

CONCLUSÃO

VII.1 - RESULTADOS OBTIDOS

Os principais resultados obtidos neste trabalho são:

i - o desenvolvimento de técnicas com o objetivo de detectar e recuperar falhas transientes e permanentes, técnicas de chaveamento de módulos, isolamento de módulos defeituosos, etc, e o desenvolvimento de uma metodologia de observação do sistema com o objetivo de obter dados para futuros estudos. Muitas destas técnicas já foram implantadas no sistema e demonstraram ter uma ótima eficiência;

ii - escolha e aplicação de um modelo geral (1) na determinação da disponibilidade do sistema. Este modelo trata as falhas transientes e permanentes de uma forma homogênea. Além disto, usamos o modelo numa aplicação sugerida pelo próprio autor: cálculo da disponibilidade de um sistema reparável;

iii - foi desenvolvido um sistema para geração de falhas transientes, contabilizando o número de falhas geradas e o número de falhas não recuperadas. Este sistema foi útil na avaliação do desempenho do sistema quando este é submetido a uma falha transiente. Este sistema mostrou ainda que as técnicas de detecção e recuperação propostas para o centro de supervisão reagem de uma forma satisfatória aos efeitos de uma falha transiente.

VII.2 - CONTINUAÇÃO DESTE TRABALHO

Como continuação deste trabalho podemos ter:

i - construção e instalação, para obter dados para futuros estudos, do Sistema de Observação do Centro de Supervisão (OO). Este dispositivo ficaria ligado "on-line" com o sistema, colhendo dados que seriam úteis, principalmente no tocante à cobertura de falhas permanentes, que não foram analisadas praticamente neste trabalho;

ii - elaboração de ferramentas computacionais com o objetivo de facilitar e automatizar o cálculo da disponibilidade e/ou confiabilidade de sistemas. útil;

iii - um estudo mais aprofundado do espectro e dos tipos de interferência a que os sistemas estão sujeitos. A partir deste estudo poderemos propor técnicas melhores de proteção para o sistema como: uma malha de aterramento, desacoplamento capacitivo para integrados, supressores de ruídos nas fontes de alimentação, blindagem para os equipamentos, etc.;

iv - estudo de novas técnicas de detecção e recuperação de falhas transientes e permanentes;

v - desenvolvimento de circuitos de chaveamento mais eficazes, para melhorar a disponibilidade de alguns subsistemas, como o subsistema de comunicação com as remotas.

vi - aperfeiçoamento do modelo usado, pois este mostrou-se deficiente para sistemas com múltipla capacidade de manutenção, ou cujo tempo de manutenção seja muito pequeno.

ANEXO I

TAXA DE FALHAS

Para estimativa da taxa de falhas dos componentes usamos as normas MIL-HDBK-217C (21).

Para cada tipo de componente existe uma fórmula que dá o valor da taxa de falhas do componente. Para circuitos integrados temos as seguintes expressões:

$$\lambda_p = \pi_Q \left[C_1 \pi_t \pi_v \pi_{pt} + (C_2 + C_3) \pi_e \right] \pi_L$$

λ_p = taxa de falha do componente

π_Q = fator de qualidade do componente

π_T = fator de aceleração por temperatura

π_V = fator de esforço devido a voltagem

π_{PT} = fator de programação (menor que 1 somente para PROMS)

π_E = fator do ambiemte

C_1, C_2 = fator de complexidade

C_3 = fator de embalagem

π_L = fator de aprendizado

As próximas tabelas mostram as taxas de falhas dos diversos componentes usados, e das várias placas do sistema.

TAXA DE FALHAS DA CPU

COMPONENTE	QUANTIDADE	UNITÁRIO	TOTAL
8088	1	0,746	0,746
2732	1	1,82	1,82
8282	51	0,21	1,05
8284	1	0,156	0,156
74132	1	0,09	0,09
8205	8	0,118	0,944
8185	17	1,27	21,59
2141	5	0,85	4,25
cristal	1	0,2	0,2
diodo	1	0,036	0,036
cap.eletrol	2 (1uF)	0,024	0,048
cap.poliester	2	0,0086	0,0172
resistor	1	0,016	0,016
chave	1	0,011	0,011
ligações	400	0,00000375	0,0015
conector 70	1	0,14	0,14
soquetes	39	0,0091	0,355
total			31,47f/Mh

TAXA DE FALHAS DA INTERFACE

COMPONENTE	QUANTIDADE	UNITÁRIO	TOTAL
SIO	1	0,584	0,584
8259	1	0,584	0,584
8251	1	0,584	0,584
8253	3	0,584	1,752
8282	2	0,21	0,42
7485	2	0,129	0,258
7421	1	0,086	0,086
8286	1	0,2	0,2
7400	5	0,09	0,45
7402	1	0,09	0,09
7474	6	0,0965	0,579
8205	2	0,118	0,236
74121	2	0,094	0,188
7404	5	0,091	0,455
74180	1	0,0992	0,0992
1488	1	0,136	0,136
1489	1	0,136	0,136

(cont)

COMPONENTE	QUANTIDADE	UNITÁRIO	TOTAL
7407	2	0,091	0,182
7410	1	0,09	0,09
7414	1	0,091	0,091
7420	1	0,086	0,086
74123	1	0,122	0,122
Resistor	11	0,016	0,176
Cp Poliester	2	0,0086	0,0172
Cpacitor	1(1uf)	0,024	0,024
Eletrolítico	3(100uf)	0,060	0,06
	1(1uf)	0,078	0,078
Diodo	1	0,036	0,036
ligações	400	0,00000375	0,0015
conector 70	1	0,14	0,14
conector 25	1	0,0214	0,0214
soquetes	42	0,0084	0,351
regulador	3	0,151	0,453
total			8,77f/Mh

TAXA DE FALHAS PLACA DE CHAVEAMENTO DE OR

COMPONENTE	QUANTIDADE	UNITÁRIO	TOTAL
H11 F1	16	0,209	3,344
7407	8	0,091	0,728
7474	4	0,0965	0,386
74123	61	0,122	0,732
8205	1	0,118	0,118
Capacitor Eletrolítico	5(470uf)	0,078	0,39
C poliester	3	0,0086	0,0258
resistor	23	0,016	0,368
soquetes	40	0,0082	0,328
ligações	320	0,00000375	0,0012
conector 70	1	0,14	0,14
conector 25	2	0,0214	0,0428
regulador	1	0,151	0,151
total			6,75f/Mh

TAXA DE FALHAS DA VGI/PARA 1 MÓDULO

COMPONENTE	QUANTIDADE	UNITÁRIO	TOTAL
transformador	1	0,0048	0,0048
transistor	1	0,11	0,11
diodo	2	0,036	0,072
1488	1	0,136	0,136
1489	1	0,136	0,136
7406	1	0,091	0,091
7400	1	0,09	0,09
7404	1	0,091	0,091
7474	1	0,00965	0,0965
ligações	40	0,00000375	0,00015
soquetes	5	0,0082	0,041
total			0,87f/Mh

TAXA DE FALHAS DO RETIFICADOR/FILTRO

COMPONENTE	QUANTIDADE	UNITÁRIO	TOTAL
transformador	1	0,053	0,053
diodo	8	0,004	0,032
C poliester	4	0,036	0,144
indutor	2	0,004	0,008
chave	1	0,011	0,011
fusível	3	0,1	0,3
C eletrolítico	3(s=0,3)	0,125	0,125
C eletrolítico	3(s=0,8)	0,413	0,826
total			1,5f/Mh

PLACA DE EXTENSÃO DE MEMÓRIA DO OC (32kb)

COMPONENTE	QUANTIDADE	UNITÁRIO	TOTAL
8185	32	1,27	40,64
2141	8	0,85	6,8
8205	8	0,118	0,944
8282	1	0,21	0,21
8286	1	0,2	0,2
7400	1	0,09	0,09
7420	1	0,086	0,086
soquetes	52	0,0089	0,4628
ligações	470	0,00000375	0,001575
conector 70	1	0,14	0,14
total			50,52f/Mh

TAXA DE FALHAS DE UM OPERADOR

Vamos considerar um operador com 16 kbytes de memória e uma placa de ITF.

TFop = TFcpu + TFitf = 31,47 + 8,77 = 40,24 f/Mh

Por simplicidade de cálculo e para compensar alguns elementos que não tenham sido considerados adotaremos:

TFop = 50 f/Mh

Que é equivalente a aproximadamente uma falha a cada dois anos e três meses.

TAXA DE FALHAS DE OC

Usaremos a configuração atual do Oc - 1 placa de operador (CPU + ITF) com 2 placas de extensão de memória.

TFcpu = TFop + 2 x TFm = 40,24 + 2 x 50,52 = 141,28 f/Mh

Usaremos:

TFcpu = 150 f/Mh

TFoc = TFcpu + 2 x TFisc + TFdisco

TFoc = 150 + 2 x 100 x 100 = 450 f/Mh

TFoc = 450 f/Mh

Por falta de dados dos fabricantes, sobre o MTBF dos equipamentos usados, faremos as seguintes hipótese sobre as taxas de falhas destes:

Modem (1200) = 50f/Mh (1f em 2 anos)
Modem (4800) = 100f/Mh

Isc = 100f/Mh (1f/ano)
Disco = 100f/Mh
Impressora = 100f/Mh
canal = 500f/Mh

obs: a taxa de falha mêdia de um canal de comunicações foi obtida de uma estatîstica feita por FURNAS entre Maio/1980 à Abril/1981.

ANEXO II

LINGUAGEM DE MÓDULOS ESTRUTURADOS (LME)

Esta linguagem foi derivada de uma linguagem de análise estruturada (21,22). Ela é uma forma gráfica de se exprimir os requisitos (ou funções) que um determinado projeto deve atender. Ela baseia-se em uma análise do tipo "top-down" do sistema, como mostra o diagrama da figura (AII.1). A partir de uma especificação global do sistema, abre-se este sistema em blocos com níveis de detalhamento cada vez maior.

Esta linguagem é composta de blocos que representam as funções que serão implementadas. Dentro de cada bloco temos o nome da função que ele representa, com as seguintes interfaces: entradas da função, saídas produzidas, controles que funcionam como se fossem parâmetros para estas funções e os mecanismos que serão usados na implementação da função (ex: mecanismos de "hardware", "software" etc.). Os blocos são interligados por setas que representam o fluxo de informação e a interconexão entre função.

A figura (AII.2) mostra um exemplo da representação de uma função em três níveis de detalhamento.

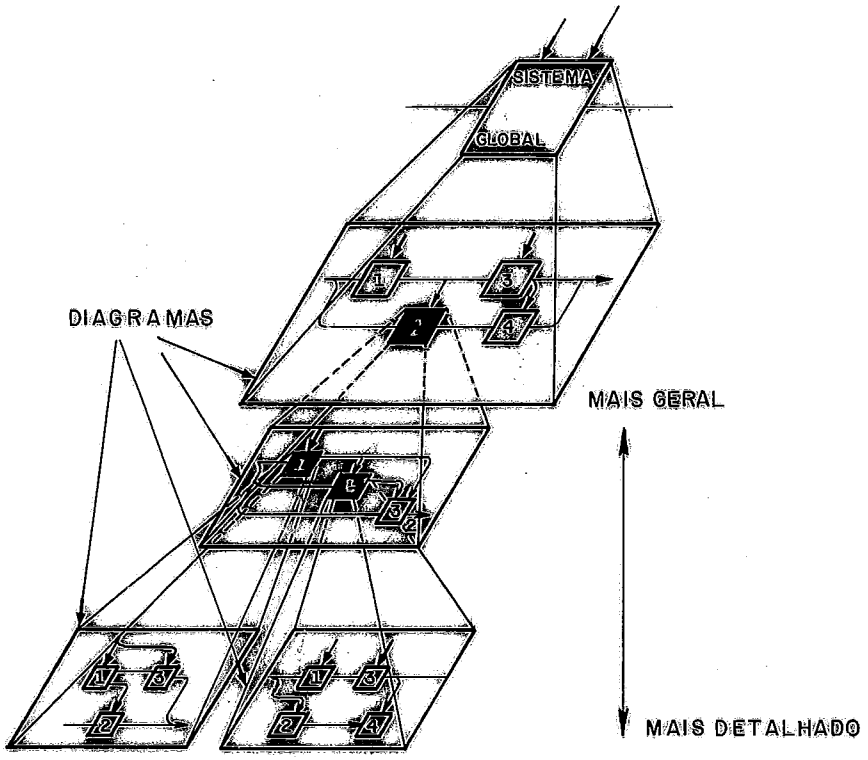


FIGURA (A.II.1) – ANÁLISE " TOP DOWN "

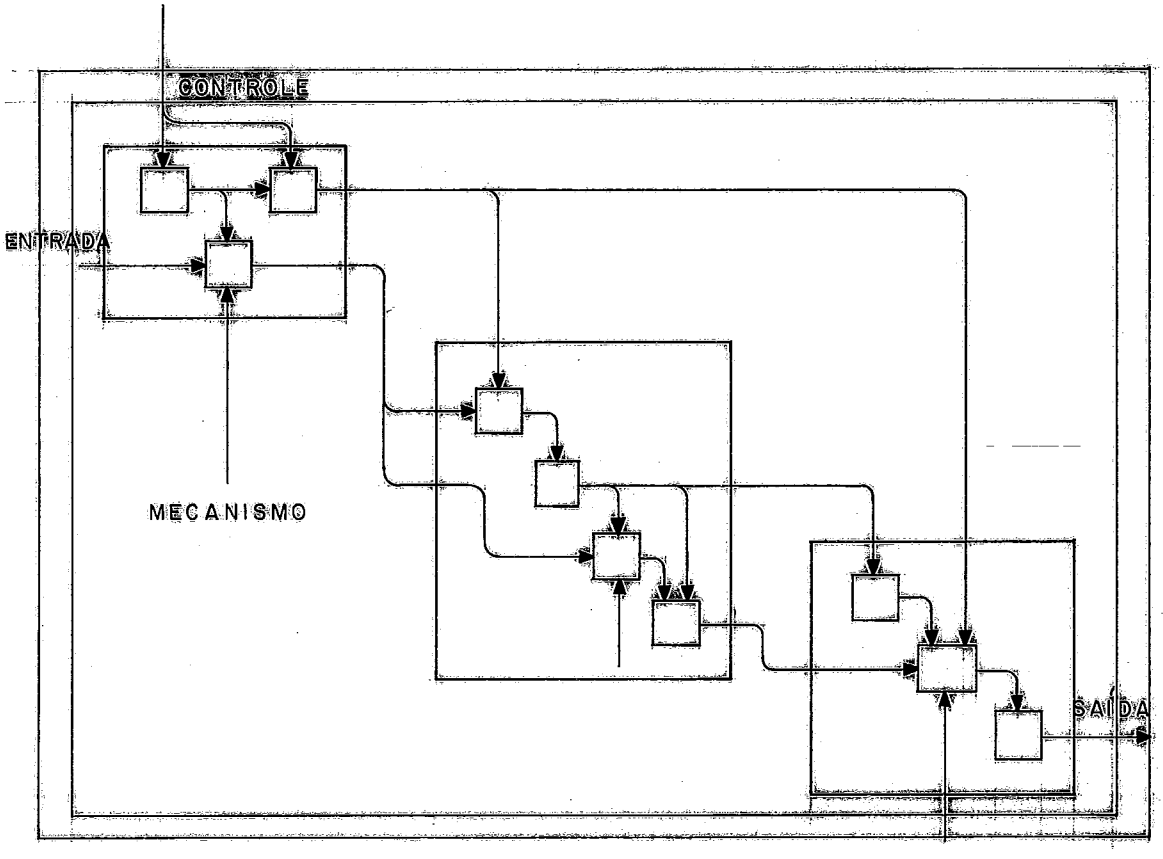


FIGURA (A III . 2) _ VISTAS DE UMA FUNÇÃO

ANEXO III

PROCESSOS MARKOVIANOS

De um modo geral, um processo estocástico é um processo Markoviano no se: a probabilidade do processo ocupar o próximo estado depende exclusivamente do estado atual, os estados passados não tem influência no futuro.

$$P[X(t_n) \leq x_n \mid X(t_{n-1}) = x_{n-1}, \ldots X(t_1) = x_1] =$$

$$P[X(t_n) \leq x_n \mid X(t_{n-1}) = x_{n-1}]$$

Um processo Markoviano discreto no tempo é determinado quando as probabilidades das transmissões são conhecidas.

$$P_{ij}(n, n+1) = P[X(t_{n+1}) = j \mid X(t_n) = i]$$

Este processo é chamado de uma cadeia de Markov. Uma cadeia de de Markov é homogênea se as probabilidades de transição não se modificarem com o tempo.

$$P_{ij}(n + m, n + m+1) = P[X(t_n + m+1) = j \mid X(t_{n+m}) = i] =$$

$$P[X(t_{n+1}) = j) \mid X(t_n) = i] = p_{ij}$$

Para um processo Markoviano contínuo no tempo, esta propriedade torna-se:

$$P_{ij}(t, t+dt) = \lambda_{ij} dt + \sigma_{dt}$$

onde:

dt - é um instante de tempo infinitamente pequeno

λ_{ij} - representa a transição entre os estados i e j

Usando a equação de CHAPMANN-KOMOLGOROV temos:

$$\dot{P}(t) = \lambda . P(t)$$

ou

$$\begin{bmatrix} \frac{dp_1(t)}{dt} \\ \frac{dp_2(t)}{dt} \\ \vdots \\ \frac{dp_n(t)}{dt} \end{bmatrix} = \begin{pmatrix} \lambda_{11} & \lambda_{12} & \cdots & \lambda_{1n} \\ \lambda_{21} & \lambda_{22} & \cdots & \lambda_{2n} \\ \vdots & \vdots & & \vdots \\ \lambda_{n1} & \lambda_{n2} & \cdots & \lambda_{nn} \end{pmatrix} \cdot \begin{bmatrix} p_1(t) \\ p_2(t) \\ \vdots \\ p_n(t) \end{bmatrix}$$

Quando $t \longrightarrow \infty$ a equação de CHAPMANN-KOMOLGOROV torna-se:

$$0 = \Pi . \lambda \qquad (1)$$

onde:

$$\Pi = [\pi_i] \quad , \quad \pi_i = \lim_{t \longrightarrow \infty} p_i(t)$$

Para resolver a indeterminação usamos a relação:

$$\sum_{i=1}^{n} \pi_i = 1 \qquad (2)$$

Para nossa aplicação, a disponibilidade do sistema é a probabilidade do sistema não estar no estado de pane, em t quando $t \longrightarrow \infty$. Consirando o estado de pane como sendo o estado n temos:

$$A = 1 - \lim_{t \longrightarrow \infty} p_n(t)$$

Das equações (1) e (2) podemos determinar o valor do $\lim_{t \longrightarrow \infty} p_n(t)$; consequentemente o valor de A

ANEXO IV

DESENVOLVIMENTO DAS EQUAÇÕES DO CAPÍTULO V

A.1 - Equação V.1

A partir do modelo da figura (V.9) obtivemos as seguintes equações:

$$-n\lambda p_0 + \psi p_1 + \psi p_2 + \ldots + \psi p_S + \psi p_{S+1} = 0$$

$$n\lambda p_0 - ((n+1)\lambda + \psi)\, p_1 + 0 \ldots + 0 = 0$$

$$0 + (n-1)\lambda p_1 - ((n-2)\lambda + \psi)p_2 + 0 \ldots + 0 = 0$$

$$0 + 0 + (n-2)\lambda p_2 - ((n-3)\lambda + \psi)p_3 + \ldots + 0 = 0$$

$$\vdots$$

$$0 + 0 + \ldots + (n-S+1)\lambda p_{S-1} - ((n-S)\lambda + \psi)p_S + 0 = 0$$

$$0 + 0 + \ldots + (n-S)\lambda p_S - \psi p_{S+1} = 0$$

$$P_0 + P_1 + P_2 + \ldots + P_S + P_{S+1} = 1$$

Da última equação temos:

$$P_1 + P_2 + P_3 + \ldots P_S + P_{S+1} = 1 - P_0$$

Substituindo os valores sucessivamente a partir da primeira equação temos:

$$-n\lambda P_0 + \psi(P_1 + P_2 + \ldots + P_S + P_{S+1}) = 0$$

$$-n\lambda P_0 + \psi(1 - P_0) = 0$$

$$P_0 = \frac{\psi}{n\lambda + \psi}$$

$$P_1 = \frac{n\psi}{(n+1)\lambda + \psi} P_0 = \frac{n\lambda}{(n\lambda + \psi)((n-1)\lambda + \psi)} \psi$$

$$P_3 = \frac{n(n-1)(n-2)\lambda^3}{(n\lambda + \psi)((n-1)\lambda + \psi)((n-2)\lambda + \psi)((n-3)\lambda + \psi)} \psi$$

$$\vdots$$

$$P_S = \frac{n(n-1)(n-2) \ldots (n-S+1)\lambda^S}{(n\lambda+\psi)((n-1)\lambda + \psi) \ldots ((n-S)\lambda + \lambda)} \psi$$

$$P_{S+1} = \frac{(n-S)\lambda}{\psi} P_S$$

$$P_{S+1} = \frac{n(n-1)(n-2) \ldots (n-S+1)(n-S)\lambda^{S+1}}{\psi(n\lambda + \psi)((n-1)\lambda + \psi) \ldots ((n-S)\lambda + \psi)} \psi$$

$$P_{S+1} = \frac{\prod_{i=0}^{S} [(n-i)\lambda]}{\prod_{i=0}^{S} [(n-i)\lambda + \psi]}$$

Como:

$$A = 1 - P_{S+1}$$

$$A = 1 - \frac{\prod_{i=0}^{S} [(n-i)\lambda]}{\prod_{i=0}^{S} [(n-i)\lambda + \psi]}$$

A.2 - Equação V.4

Usando o modelo da figura (V.13) temos:

$$-[n\lambda(1-c) + (n+1)c\lambda + \lambda(1-c)]P_1 + \psi P_2 + \psi P_4 = 0 \qquad (1)$$

$$(n+1)c\lambda p_1 - (n\lambda + \psi)P_2 = 0 \qquad (2)$$

$$\lambda(1-c)P_1 - n\lambda P_3 = 0 \qquad (3)$$

$$P_1 + P_2 + P_3 + P_4 = 1 \qquad (4)$$

$$(2) \qquad P_2 = \frac{(n+1)\lambda c}{(n\lambda + \psi)} P_1$$

$$(3) \qquad P_3 = \frac{(1 - c)}{\psi} P_1$$

$$(1) \qquad P_1 = \frac{\psi(n\lambda + \psi)}{\lambda(n + 1)(n\lambda + \psi - c\psi)} P_4$$

Substituindo tudo em (4)

$$P_4 = \frac{n(n + 1)(n\lambda + \psi - c\psi)\lambda}{(n(n+1)\lambda + n\psi - \psi(1 - c))(n\lambda + \psi)}$$

$$A = 1 - \frac{n(n+1)(n\lambda + \psi - c\psi)\lambda}{(n(n+1)\lambda + n\psi + \psi(1-c))(n\lambda + \psi)}$$

A.3 - Equação V.7

Usando o modelo da figura (V.14) temos:

$$-3\lambda P_1 + \psi P_2 + \psi P_3 + \psi P_4 = 0 \qquad (1)$$

$$3\lambda c P_1 - (2\lambda + \psi) P_2 = 0 \qquad (2)$$

$$2\lambda c P_2 - (\lambda + \psi) P_3 = 0 \qquad (3)$$

$$P_1 + P_2 + P_3 + P_4 = 1 \qquad (4)$$

$$(2) \quad P_2 = \frac{3\lambda\psi}{2\lambda + \psi} P_1$$

$$(3) \quad P_3 = \frac{6\lambda^2 c^2}{(\lambda+\psi)(2\lambda+\psi)} P_1$$

(4) $(P_2 + P_3 + P_4) = 1 - P_1$

(1) $$P_1 = \frac{\psi}{3\lambda + \psi}$$

$$P_2 = \frac{3\lambda c\psi}{(2\lambda + \psi)(\lambda + \psi)}$$

$$P_3 = \frac{6\lambda^2 c^2 \psi}{(3\lambda + \psi)(2\lambda + \psi)(\lambda + \psi)}$$

Substituindo tudo em 4 termos:

$$A = 1 - \frac{6\lambda^3 + 6\lambda^2\psi - 6\lambda^2\psi c + 3\lambda\psi(\lambda + \psi) - 3\lambda\psi c(\lambda + \psi)}{(3\lambda + \psi)(2\lambda + \psi)(\lambda + \psi)}$$

BIBLIOGRAFIA

1 - NG, Ying W. - "Reliability Modeling and Analysis for Fault-Tolerant Computer", Dep. Comput. SCI. Univ. California, Los Angeles, Tech. Rep. UCLA-Eng-7698. Setembro/1976.

2 - Avizienis, A. - "Arquitecture of Fault-Tolerant Computing Systems", Int. Symp. Fault-Tolerant Computing, Paris, França - Junho/1975 - páginas: 3-16.

3 - Avizienis, A. - "Fault-Tolerant Systems", IEEE - Transactions on Computers, Vol. C-25 n 12, Dezembro/1976 - páginas: 1304-1312.

4 - Avizienis, A - "Fault-Tolerant: The Survival Attribute of Digital Systems" - Proceedings of the IEEE, Vol. 66, n 10, Outubro/1978 - páginas: 1109-1125.

5 - Laprie, J.C. - "Prévision de la Sûreté de Fouctionnement et Architecture de Structures Numériques Temps Réel Réparables", Thése de Doctorat - és - Sciences, Université Paul Sabatier, Toulouse, 1975.

6 - Moszkowicz, Maurício - "Análise e Implementação de Técnicas Associadas à Confiabilidade de um Terminal de Aquisição de Dados", Tese de Mestrado, Coppe/UFRJ, Novembro/1978.

7 - Brown Boveri -"Load Dispatching Systems", Brown Boveri Review, Vol. 66, Março/1979, Baden/Suíça, páginas: 145-236.

8 - Narita, S. - Hamman, M.S.A.A. - "Reliability Evaluation of Hierarchical Power Control Systems and Design of Component Redundances", IEEE Transactions or Power Apparatus and Systems, Vol. PAS-95, n 3, Maio-Junho/1976, páginas: 918-926.

9 - Fernandes, A.L.B. - "Centro de Operação Regional Análise de Requisitons", Relatório Técnico CEPEL.

10 - Fernandes, A.L.B. - "Redes Locais de Controle Distribuído: Sua perspectiva frente o quadro nacional", relatório técnico CEPEL.

11 - Fernandes, A.L.B., - Andrade, H.G. - Appel, O - Freitas, C.A.B. - Garrofé, P.H.S. - "Projetos de Centros de Supervisão de Sistemas de Energia Elétrica", VI SNPTEE, Grupo V, Balneário Camboriú/SC - 1981.

12 - Fernandes, A.L.B. - Terry, L.A. - Appel, O. - Moszkowicz, M. - Garcia, J. - Costa, R.S. - Lopes, J.M.R. - Andrade, H. G. - "Centros de Supervisão para sistemas Elétricos", V SNPTEE, Grupo V, Recife/PE, Novembro/1979.

13 - Fernandes, A.L.B. - "Manual de Hardware do Protótipo de Centro de Supervisão Regional para Furnas Centrais Elétricas S.A." - Relatório Técnico CEPEL.

14 - INTEL-"RMX USERs Guide".

15 - Gracia, J. -"Desenvolvimento de uma Rede de Microprocessadores Aplicada a Supervisão de Sistemas Elétricos",Tese de Mestrado, COPPE/UFRJ, Dezembro/1980.

16 - Metcalfe, R.M. & Boggs, D.R. - "Ethernet: Distributed Packet Switching for Local Computer Networks", Communications of the ACM, Vol. 19, n 7, Julho/1976, página: 395-404.

17 - Shoch, J.F. & Hupp, J.A. - "Measured Performance of an Ethernet Local Network", Communications of the ACM, vol.23, n 12, Dezembro/1980, páginas: 711-721.

18 - Menascé, D.A. & Schwabe, D. - "Redes de Computadores (Aspectos Técnicos e Operacionais)", Terceira Escola de

Computação, Departamento de Informática/PUC-RJ, Rio de Janeiro/1982.

19 - Costa, R.S. - "Projeto e Construção de um Centro de Supervisão Baseado em uma Arquitetura Distribuída" - tese de Mestrado, Coppe/UFRJ, de Dezembro/1980.

20 - Andrade, Homero G.,"Operador de Master", relatório técnico CEPEL.

21 - NG, Ying W. - Avizienis, A. - "A Unified Reliability Model for Fault-Tolerant Computers", IEEE Transactions on Computers, Vol. C-29, n 11, Novembro/1980, páginas: 1002-1011.

22 - NG, Ying W - Aviziens, A. - "A Unifying Reliability Model for Colosed Fault-Tolerant Systems", Dig. 5th Int. Symp. on Fault - Tolerant Comput., Paris/França, Junho/1975, página: 224.

23 - NG, Ying W. - Avizienis, A. -"A Model for Gracefully Degrading and Repairable Fault-Tolerant Systems", Proc. 7th Int. Conf. on Fault-Tolerant Computer, Los Angeles/CA, Junho/1977, páginas: 22-28.

24 - Merryman, P.M. - Avizienis, A. -"Modeling Transienis in TMR Computers Systems" - Proc. Annual Reliability and Mantainability Symposium, 1975, páginas: 333-334.

25 - Arnold, Thomas F. - "The Concept of Converage and Its Effect on the Reliability Model of a Repairable System", IEEE Transactions on Computers, vol. L-22, n 3, Março/1973, páginas: 251-254.

26 - Anderson, J. - Randell, B. - "Computing Systems Reliability", Cambrige University Press, Cambrige Londres.

27 - Fernandes, A.L.B. - Moszkowicz, M. - Valle, L. D. - "Metodologia para Desenvolvimento de Software em Sistemas

Distribuídos", SUCESU, Rio de Janeiro, Outubro/1982.

28 - Intel - "MCS-86 USERs Manual"