1. Publicação nº	2. Versão	3. Data	5. Distribuição
INPE-3933-TDL/227		*Junho, 1986*	☐ Interna ☒ Externa ☐ Restrita

4. Origem	Programa
DRH/DCA	*FRH/ECO*

6. Palavras chaves - selecionadas pelo(s) autor(es)

PROCESSADOR DE COMUNICAÇÃO — *DISPONIBILIDADE*
CONFIABILIDADE — *TOLERÂNCIA A FALHAS*

7. C.D.U.: *681.3.012-192*

8. Título *INPE-3933-TDL/227*

UMA ARQUITETURA COM MECANISMOS DE TOLERÂNCIA A FALHAS PARA O MULTIPROCESSADOR DE COMUNICAÇÃO EM REDE - MCR

10. Páginas: *162*

11. Última página: *D.5*

12. Revisada por

Alderico R. de P. Junior

9. Autoria

Antonio Esio Marcondes Salgado

Assinatura responsável

13. Autorizada por

Marco Antonio Raupp
Diretor Geral

14. Resumo/Notas

Neste trabalho é feita a análise do equipamento Multiprocessador de Comunicação em Rede (MCR), em sua configuração atual, relativa à sua confiabilidade e disponibilidade. Em seguida é proposta uma nova arquitetura com mecanismos de tolerância a falhas, visando uma melhoria nestes parâmetros. A concepção desta nova arquitetura tem como princípio a utilização dos circuitos já existentes, com modificações mínimas quando necessário. Por fim, os valores obtidos para a confiabilidade e disponibilidade são comparados com os valores atuais para haver uma visão dos benefícios alcançados.

15. Observações *Dissertação de Mestrado em Eletrônica e Telecomunicações - Opção Sistemas Digitais e Analógicos aprovada em dezembro de 1985.*

Aprovada pela Banca Examinadora
em cumprimento a requisito exigido
para a obtenção do Título de Mestre
em Eletrônica e Telecomunicações

Dr.Eduardo Whitaker Bergamini — Presidente

Dr.Alderico Rodrigues de Paula Jr. — Orientador

Engº Mauro Hissao Hashioka, Mestre — Co-Orientador

Dr.Jorge Moreira de Souza — Membro da Banca -convidado-

Dr.Tatuõ Nakanishi — Membro da Banca

Candidato: Antonio Ésio Marcondes Salgado

São José dos Campos, 09 de dezembro de 1985

ABSTRACT

In this work an analysis of the Network Communication Multiprocessor (MCR) concerning its availability and reliability parameters is presented. A new configuration including fault tolerant mechanisms is proposed in order to have better values to these parameters. The basic design goal of this new architecture is to use the available hardware with minimal modifications. Finally, the values of availability and reliability of the proposed architecture are compared with the existing ones in order to show the benefits obtained.

AGRADECIMENTOS

Meus sinceros agradecimentos a todos que colaboraram direta e indiretamente na execução deste trabalho, em especial ao Dr. Alderico Rodrigues de Paula Jr. pela orientação, incentivo e interesse durante todas as fases de desenvolvimento do presente trabalho, e ao Engº Mauro Hissao Hashioka pelo trabalho de co-orientação que resultou em inúmeras contribuições.

SUMÁRIO

Pág.

Pág.

LISTA DE FIGURAS

Pág.

Pág.

LISTA DE TABELAS

CAPÍTULO 1

INTRODUÇÃO

As redes de computadores surgiram a partir da idéia de partilhar recursos entre dois ou mais computadores. Desta maneira, um computador mesmo não tendo capacidade de resolver certos problemas, poderia solucioná-los utilizando recursos de outros computadores.

A ligação entre dois ou mais computadores requer um conjunto de regras básicas denominado protocolo, ao qual os computadores devem obedecer para se interconectarem.

A grande maioria das redes de computadores é dividida em dois conjuntos distintos: o conjunto das máquinas que executam os programas aplicativos, denominadas hospedeiros da rede, e o conjunto de máquinas responsáveis pela comunicação entre hospedeiros. A este conjunto de máquinas responsáveis pela comunicação dá-se o nome de sub-rede de comunicação de dados.

O protocolo de comunicação é implementado tanto nos hospedeiros como na sub-rede de comunicação. A sub-rede é formada por nós de chaveamento, onde se encontram computadores dedicados única e exclusivamente a prover mecanismos que viabilizem o transporte de dados entre dois hospedeiros da rede, tais como: roteamento de dados, controle de fluxo, correção de erros, armazenamento temporário de dados, etc. Nestes nós de chaveamento estão ligados os hospedeiros e terminais da rede. Um nó é conectado a outro utilizando os diversos meios de comunicação existentes, tais como: cabo coaxial, linhas telefônicas, fibra ótica, etc.

Os nós de chaveamento de uma rede de computadores geralmente são computadores dedicados ao tratamento de informações em linhas seriais. O modo como estas informações trafegam entre os nós varia de rede para rede.

A função dos processadores de comunicação ou processadores de chaveamento (nós de rede) depende da organização da rede a qual ele está incorporado e do tipo de serviço que é oferecido ao usuário. Aos nós da rede são ligados os computadores hospedeiros e/ou terminais.

O comportamento de uma rede de computadores pode ser abordado sob diversos aspectos, tais como capacidade de atendimento às solicitações de transporte de dados, fluxo de dados permitido, retardo médio no transporte de dados, confiabilidade da sub-rede, etc.

O parâmetro confiabilidade da sub-rede é obtido a partir da confiabilidade dos diversos equipamentos que a compõem e envolve um estudo das taxas de falhas de cada um destes equipamentos. A falha em um determinado processador de chaveamento ou nó pode bloquear o acesso de diversos usuários à rede, bem como prejudicar o fluxo de dados na sub-rede de comunicação, degradando o desempenho da rede de computadores.

Este trabalho analisa a configuração atual do "Multiprocessador de Comunicação em Rede" (MCR) sob o aspecto de confiabilidade e tolerância a falhas. O MCR é um equipamento desenvolvido pelo Departamento de Engenharia e Computação em Aplicações Espaciais (DCA) do INPE para atuar como processador de chaveamento nos sistemas REDACE e RECODI. O desenvolvimento deste equipamento já foi analisado, com relação ao retardo médio e ao fluxo de dados, por Hashioka (1983) e Pires (1983). O objetivo deste trabalho é ser uma extensão do trabalho já feito, na qual, uma vez analisado o comportamento atual do MCR, é feita uma proposta de alteração em sua configuração, visando aumentar sua confiabilidade e disponibilidade, incluindo mecanismos de tolerância a falhas.

O Capítulo 2 introduz os conceitos básicos da teoria de confiabilidade e apresenta alguns equipamentos de aplicação semelhante ao MCR, os quais utilizam mecanismos de tolerância a falhas.

O equipamento MCR é apresentado no Capítulo 3 onde é feita uma análise da atual arquitetura com respeito à confiabilidade/disponibilidade.

O Capítulo 4 contém a proposta de arquitetura para o equipamento MCR, prevendo mecanismos de tolerância a falhas e a análise da disponibilidade obtida com esta nova arquitetura.

As conclusões sobre os resultados obtidos são apresentadas no Capítulo 5.

CAPÍTULO 2

CONFIABILIDADE E SUAS APLICAÇÕES

2.1 - INTRODUÇÃO À CONFIABILIDADE

Ao projetar uma rede de computadores, certos requisitos devem ser satisfeitos de modo a garantir um serviço adequado aos usuários. A rede deve operar durante o maior tempo possível sem que ocorram interrupções prolongadas na operação. Para que este objetivo seja atingido, é necessária uma especial atenção à confiabilidade e à tolerância a falhas dos equipamentos que compõem a rede.

Equipamentos confiáveis (com baixa probabilidade de falha) custam caro, pois exigem redundância nos diversos circuitos e/ou uso de componentes mais sofisticados. Uma vez ocorrida a falha, outro parâmetro toma grande importância: o tempo de reparo. Para que este tempo seja reduzido é necessário pessoal técnico bem treinado, bem como métodos e equipamentos adequados para a manutenção.

A equação abaixo demonstra o custo de um equipamento na rede (Cooper, 1977):

$$Ct = Co + Cf \cdot N,$$

onde Ct é o custo total durante um certo período de tempo, Co o custo total durante este mesmo período de tempo, considerando que não haja falhas, Cf o custo médio para o reparo do equipamento quando ocorre uma falha e N o número de falhas que ocorrem no tempo considerado.

O fator N é função da confiabilidade do equipamento. Para reduzi-lo seria necessário um novo projeto, o que acresceria o custo inicial Co, fazendo supor que uma confiabilidade maior implica um equipamento mais caro. É freqüentemente mais fácil reduzir Cf, o qual é função da manutenção; neste caso considerada como a adaptabilidade de equipamentos para detecção e reparo de falhas. Somado a estes fato

res existem as perdas de lucro que a inatividade do equipamento provoca, já que as taxas em uma rede são cobradas de acordo com o tempo de serviço prestado ao usuário.

Intuitivamente pode-se concluir que a melhora do serviço de reparo e a conseqüente queda no custo desta operação sejam consequências da experiência adquirida depois da ocorrência de inúmeras falhas, sanadas por uma equipe técnica própria ou por uma equipe técnica pertencente a terceiros, que tenham experiência neste campo.

Para o usuário do equipamento de comunicação de dados, a confiabilidade torna-se um fator importante no projeto e operação da rede de comunicação de dados. O conhecimento da confiabilidade das subunidades do sistema provê uma ajuda significativa ao definir a disponibilidade da rede, a característica de manutenção e a estratégia de operação, bem como uma maneira de obter um custo baixo que atenda às necessidades dos usuários.

A confiabilidade de um sistema pode ser caracterizada pela função R(t), a qual expressa a probabilidade de um sistema operar dentro de determinadas especificações durante um período de duração "t", dado que em "t=0" o sistema estava operando corretamente.

O cálculo da confiabilidade de um sistema permite a avaliação de seu desempenho com respeito à disponibilidade do equipamento e outras estimativas que podem ser úteis ao projetista e ao usuário. Através dos valores obtidos com estes cálculos, sabe-se se a máquina ou sistema projetado atende às exigências mínimas para operar com resultados satisfatórios.

Um parâmetro importante para calcular a confiabilidade de um sistema é a taxa de falhas que este apresenta. A falha em um sistema ocorre quando o seu comportamento desvia daquele requerido pelas especificações (Anderson, 1982).

As falhas podem ser permanentes, intermitentes, se presentes apenas ocasionalmente, e transientes, se resultantes de interferência do meio ambiente.

A taxa de falhas de um sistema é calculada a partir da taxa de falhas de cada módulo que compõe este sistema. Já a taxa de falhas de cada módulo é calculada a partir da taxa de falhas de cada componente que integra este módulo.

O valor da taxa de falhas de cada componente (transistor, circuito integrado, resistores, etc.) é calculado utilizando parâmetros fornecidos pelo fabricante. Estes parâmetros estão relacionados com: processo de fabricação, material utilizado na confecção do componente, comportamento em relação à variação de temperatura, complexidade, ambiente, tensão, qualificação e maturidade.

Estatísticas feitas pelos fabricantes mostram que a taxa de falhas de um componente tem três fases distintas, que são: taxa de falhas "infantil", taxa de falhas durante a "vida útil" e taxa de falhas durante o "envelhecimento".

Os componentes eletrônicos passam por um processo de inspeção, após a fabricação, que visa detetar componentes defeituosos e separá-los antes da comercialização ou aplicação em algum sistema. Todo processo de fabricação de semicondutores produz um certo número de componentes defeituosos e, mesmo que o fabricante tenha detetado e removido estes componentes, falhas continuarão a ocorrer por um período conhecido por "mortalidade infantil". Este período é tipicamente de 20 semanas ou menos, durante o qual a taxa de falhas continua a decrescer. Ao fim deste período as falhas tendem a estabilizar em uma taxa constante durante um longo tempo, às vezes 25 anos ou mais. Por fim, a taxa de falhas tende a crescer novamente num período conhecido por "envelhecimento" (Siewiorek, 1982).

Uma técnica utilizada pelos fabricantes para contornar o problema da fase de falhas "infantil" é o procedimento de cozimento ("burn in"), no qual o componente é submetido a operações em condições severas, nas quais se inclui a alta temperatura. Este procedimento é realizado visando acelerar a passagem do período de falhas "infantil" e distribuir o componente no mercado já com características normais de "vida útil".

A curva da Figura 2.1 mostra o comportamento da taxa de falhas de um componente em função do tempo, destacando-se as três fases citadas.

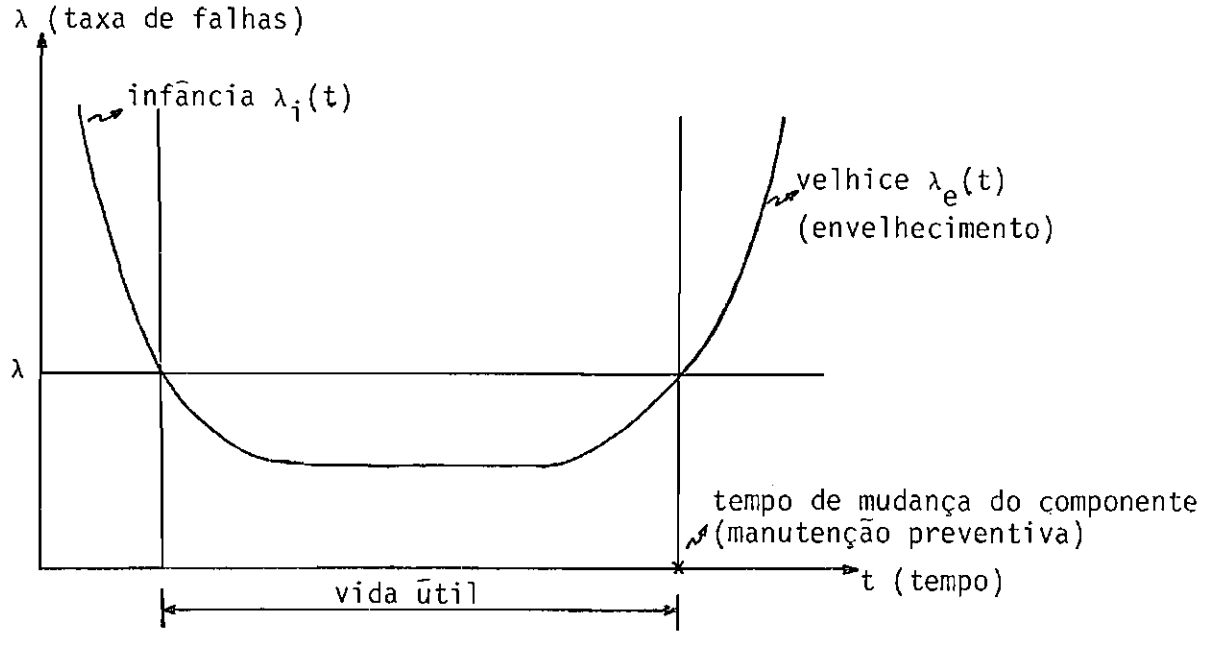


Fig. 2.1 - Comportamento da taxa de falhas de um componente.

2.2 - CRITÉRIOS PARA ANÁLISE DA CONFIABILIDADE

2.2.1 - MODELO PROBABILÍSTICO

A comparação de tolerância a falhas, de maneira a tirar conclusões aplicáveis durante a definição de um sistema, requer métodos de avaliação. Um critério de avaliação recai sobre a confiabilidade. O termo confiabilidade tem sido usado repetidamente em vários livros e artigos para descrever qualitativamente o comportamento de um componente ou sistema.

A confiabilidade de um sistema é definida em função da taxa de falhas dos componentes que compõem este sistema. Conforme a curva na Figura 2.1, a taxa de falhas de um componente ou sistema se mantém constante durante a chamada "vida útil", o que implica que a probabilidade de falha neste período é independente da idade (Toy, 1981). Isto significa dizer que um equipamento antigo que se encontra no período de "vida útil" tem o mesmo comportamento que um equipamento recém-instalado e que se encontra também no período de "vida útil". Para qualquer taxa de falhas constante o valor da confiabilidade depende somente da variável tempo.

Supondo a taxa de falhas constante, a distribuição do tempo entre falhas é caracterizada por uma exponencial negativa, que tem a seguinte forma:

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

onde λ = taxa de falhas e t = tempo.

Supõe-se que quando um sistema inicia a operação, i.é., começa sua missão em um tempo $t=0$, todos seus componentes estão operacionais. Desta maneira tem-se a confiabilidade do sistema $R(0)=1$. Considerando que o sistema deve falhar em um tempo finito, tem-se $R(\infty)=0$.

Se um sistema não contém nenhuma redundância e se as falhas nos componentes são estatisticamente independentes, então a confiabilidade do sistema, Rsis(t), é o produto das confiabilidades dos componentes do sistema:

$$Rsis(t) = \prod_{i=1}^{n} Ri(t) = \prod_{i=1}^{n} e^{-\lambda_i t} = e^{-(\sum_{i=1}^{n} \lambda_i)t} = e^{-\lambda sis\ t},$$

onde n = número de componentes e λ_i = taxa de falhas do i-ésimo componente.

A confiabilidade Rsis(t) obtida é também exponencial e a taxa de falhas para o sistema é dada por:

$$\lambda_{sis} = \sum_{i=1}^{n} \lambda_i$$

2.2.2 - PARÂMETROS DE MEDIDA EM MODELOS SIMPLES

Alguns outros parâmetros são utilizados para caracterizar a confiabilidade e disponibilidade de sistemas. Para as funções de confiabilidade utilizadas na Seção 2.2.1 tem-se:

a) "Mean Time To Failure" (MTTF): tempo médio para ocorrência de falha. Tanto para os componentes como para o sistema, o MTTF é considerado tempo esperado para ocorrência da primeira falha, dado que a operação do sistema é correta desde o instante inicial. O MTTF é dado por:

$$MTTF = \int_0^\infty R(t)\ dt$$

$$MTTF = \int_0^\infty e^{-\lambda t}\ dt$$

$MTTF = 1/\lambda$.

b) "Mean Time To Repair" (MTTR): tempo médio para reparo. É o tempo esperado para o reparo de sistemas ou sub-sistemas onde ocorrem falhas.

Dado μ = taxa média de reparo por unidade de tempo, tem-se:

$MTTR = 1/\mu$.

c) "Mean Time Between Failures" (MTBF): tempo médio entre falhas. O MTBF é o tempo médio entre falhas para sistemas que permitam o reparo, e portanto derivado dos processos de reparo e falha. O MTBF por várias vezes é considerado erroneamente como MTTF. A melhor aproximação para o MTBF é:

$MTBF = MTTF + MTTR$

$MTBF = 1/\lambda + 1/\mu$.

d) Disponibilidade ("Availability"): Entende-se por disponibilidade a porção de tempo em que o sistema está operacional (Muller, 1979).

A disponibilidade "A" de um sistema é dada por:

$$A = \frac{MTTF}{MTTR + MTTF} = \frac{\mu}{\lambda + \mu}$$

2.2.3 - MODELAGEM DE SISTEMAS

Um computador pode ser considerado um sistema formado por um conjunto de subsistemas ou sistemas de menor dimensão. Sob este ponto de vista, o menor sistema que integra o computador pode ser considerado o componente eletrônico.

A avaliação da confiabilidade de um sistema requer uma avaliação preliminar da confiabilidade de cada subsistema que compõe este sistema. A confiabilidade do sistema como um todo é função da confiabilidade de cada subsistema e de que maneira estes subsistemas são combinados.

É importante que, nos diversos modelos analisados, seja caracterizada a independência entre os subsistemas, ou módulos, que compõem o sistema. Desta maneira, cada subsistema pode ter sua taxa de falhas tratada particularmente. A taxa de falhas do sistema é uma função das taxas de falhas dos subsistemas que o compõem.

Os módulos que compõem um sistema podem ser modelados em série, em paralelo, numa combinação em série/paralelo etc. Podem estar todos ativos, alguns ativos e outros não e ter ou não chaveamento entre eles.

A configuração de um sistema adquire diversas formas de acordo com sua finalidade. O uso de módulos reservas é uma técnica para aumentar a confiabilidade de um sistema (assunto tratado na Seção 2.3), e estes módulos devem ser considerados por ocasião da modelagem do sistema, bem como deve ser considerado se há ou não chaveamento entre os módulos ativos e reservas.

a) Sistemas em série

Os módulos que compõem o sistema são modelados em série quando, para o sistema funcionar, é necessário que todos os módulos funcionem corretamente.

A Figura 2.2 mostra um modelo de sistema em série.

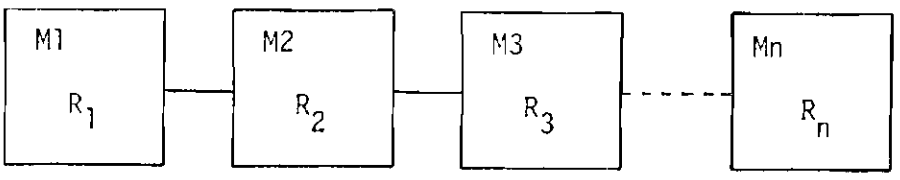


Fig. 2.2 - Modelo de sistema série.

Considerando Ri(t) a confiabilidade do módulo "Mi", e que todos os módulos são independentes, a confiabilidade do sistema é dada por:

$$Rs(t) = \prod_{i=1}^{n} Ri(t),$$

onde "n" é o número total de módulos modelados em série no sistema.

A probabilidade de falha do sistema Q(t) é a seguinte no sistema em série:

$$Qs(t) = 1-Rs(t) = 1 - \prod_{i=1}^{n} Ri(t),$$

$$Qs(t) = 1 - \prod_{i=1}^{n} (1-Qi(t)),$$

onde Qi(t) é a probabilidade de falha de cada módulo.

b) Sistemas em paralelo

Todos os módulos que compõem este sistema estão ativos e o sistema falhará por completo se todos os módulos falharem. Desta maneira os módulos são modelados em paralelo.

O sistema em paralelo puro é aquele no qual incialmente todos os módulos estão energizados no instante incial e qualquer módulo pode sustentar a operação do sistema (Kapur, 1977).

A Figura 2.3 mostra um sistema em paralelo.

Considerando Qi(t) a probabilidade de falha do módulo "Mi" e que todos os módulos são independentes, a probabilidade de falhas do sistema é dada por:

$$Qp(t) = \prod_{i=1}^{n} Qi(t),$$

onde "n" é o número de módulos modelados em paralelo do sistema.

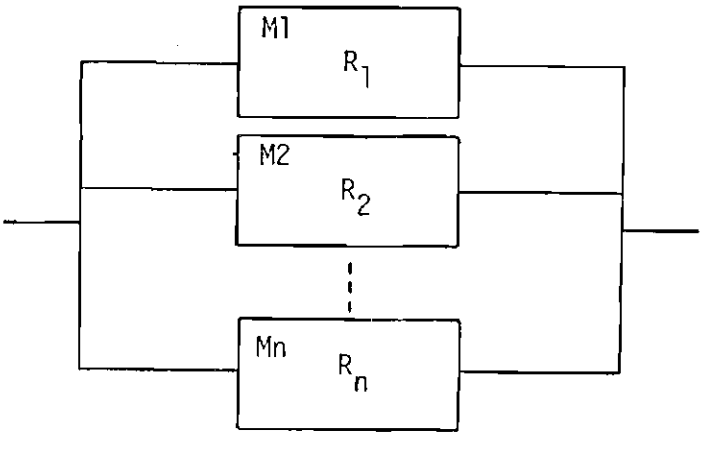


Fig.2.3 - Modelo de sistema paralelo.

A confiabilidade do sistema é dada por:

$$Rp(t) = 1-Qp(t)$$

$$Rp(t) = 1 - \prod_{i=1}^{n} Qi(t)$$

$$Rp(t) = 1 - \prod_{i=1}^{n} (1-Ri(t)).$$

Nota-se que há dualidade entre Rs(t) e Qp(t), e entre Rp(t) e Qs(t).

c) Sistemas em série/paralelo

Estes sistemas são uma combinação de sistemas em paralelo dispostos em série. Neste caso o sistema global falhará se um dos sistemas em paralelo falhar por completo.

A Figura 2.4 mostra um sistema em série/paralelo.

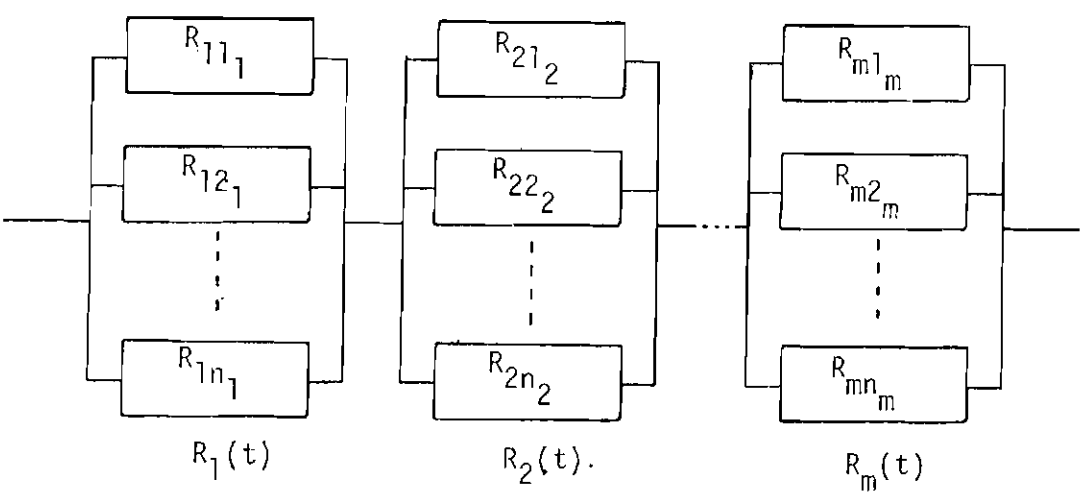


Fig. 2.4 - Modelo de sistema em série/paralelo.

A confiabilidade do sistema global é dada por:

$$Rsp(t) = \prod_{k=1}^{m} Rk(t),$$

onde Rk(t) é a taxa de falhas de cada sistema em paralelo e "n" o número de sistemas em paralelo modelados em série:

$$Rsp(t) = \prod_{k=i}^{m} \left(1 - \prod_{i=1}^{n_k} (1 - Rki(t))\right),$$

onde Rki é a confiabilidade do i-ésimo módulo do k-ésimo sistema paralelo e "n_k" o número de módulo no sistema em paralelo K.

d) Sistemas em paralelo/série

São uma combinação de sistemas série dispostos em paralelo. Neste caso o sistema global falhará se todos os sistemas série falharem.

A Figura 2.5 mostra um sistema em paralelo/série.

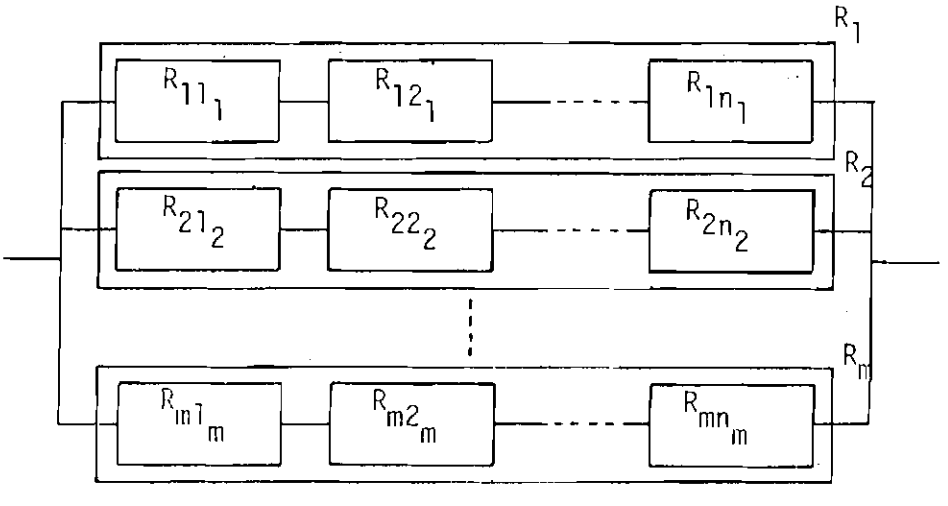


Fig. 2.5 - Modelo de sistema em paralelo/série.

A confiabilidade do sistema global é dada por:

$$Rps(t) = 1 - \prod_{k=1}^{m} (1-Rk(t)).$$

onde Rk(t) é a confiabilidade de cada sistema em série e "n" o número de sistema em série modelados em paralelo.

$$Rps(t) = 1 - \prod_{k=1}^{m} \left(1 - \prod_{i=1}^{n_k} Rki(t)\right).$$

onde Rki(t) é a confiabilidade do i-ésimo módulo do k-ésimo sistema em série e "n_k" o número de módulos neste sistema em série K.

e) Sistemas M-de-N

Generalização de sistemas em paralelo, no qual M dos N módulos, dispostos em paralelo, devem funcionar de maneira correta para que o sistema de N módulos opere corretamente.

A Figura 2.6 mostra um sistema M-de-N.

No caso particular no qual os N módulos são idênticos, i.é., têm a mesma confiabilidade Rm(t), se uma tarefa requer K módulos o sistema pode tolerar até N-M falhas. Deste modo a confiabilidade do sistema M-de-N é dada por:

$$Rs(t) = \sum_{i=0}^{N-M} \binom{N}{i} Rm^{N-i} (1-Rm)^{i} .$$

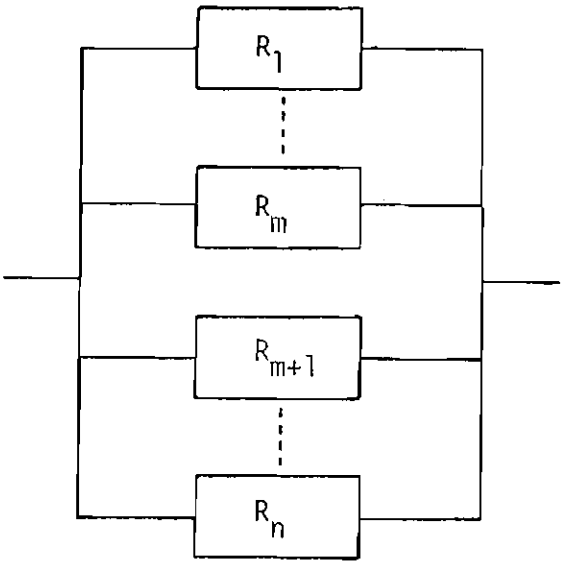


Fig. 2.6 - Modelo de sistema M-de-N.

f) Sistemas com chaveamento

São sistemas que dispõem de uma chave para mudança dos módulos ativos. Neste caso um outro parâmetro passa a fazer parte do cálculo da confiabilidade: a probabilidade "C" de o chaveamento ter sucesso. No caso de chaveamento perfeito C=1.

A Figura 2.7 mostra um sistema com um módulo ativo e "s" módulos reservas. Considerando o chaveamento perfeito (C=1), a taxa de falhas dos módulos reservas igual a zero, quando estes não estão alimentados, e a taxa de falhas dos módulos ativos igual para todos, tem-se (Kapur, 1977):

$$Rs(t) = e^{-\lambda t} \sum_{i=0}^{S} \frac{(\lambda t)^i}{i!} \quad .$$

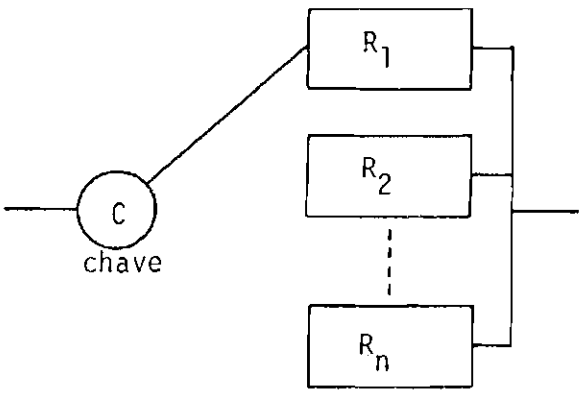


Fig. 2.7 - Sistema com chaveamento.

Um módulo reserva é energizado a partir do momento em que ele é chaveado para atuar no sistema. Enquanto não energizado sua taxa de falhas é igual a zero, e após energizado sua taxa de falhas é igual a λ, a mesma do módulo ativo que falhou.

Para "q" elementos ativos, "s" reservas e admitindo as considerações anteriores, tem-se:

$$R_s^q(t) = e^{-q\lambda t} \sum_{i=0}^{S} \frac{(q\lambda t)^i}{i!} \quad .$$

g) Modelo BCS

O modelo BCS (Bouricius, 1969) é baseado na suposição de que cada módulo tem uma taxa de falhas constante (λ quando energizado e μ quando não-energizado) e que a probabilidade de sucesso no chaveamento é constante para todos os reservas.

A fórmula recursiva abaixo foi derivada para calcular a confiabilidade de um subsistema formado por "q" módulos ativos e "s" módulos reservas:

$$ {}_cR_s^q(t,\lambda,\mu) = {}_cR_{s-1}^q(T,\lambda,\mu) + \int_0^T c^s \frac{d}{dt} [1-R_{s-1}^q(t,\lambda,\mu)] e^{-\mu t} e^{-q\lambda(T-t)} dt, $$

onde ${}_cR_s^q(T,\lambda,\mu)$ é a confiabilidade de um subsubsistema no tempo T quando "s" módulos reservas estão disponíveis.

Segundo a fórmula dada, a confiabilidade com "s" reservas é devido à operação confiável com "s-1" reservas, mais o incremento de confiabilidade devido ao "s-ésimo" reserva. Este último termo é dado pela integral no intervalo [0,T] do produto de:

1) c^s, que é a probabilidade de ocorrência de "s" recuperações (chaveamento com sucesso);

2) $\frac{d}{dt} [1-R_{s-1}^q(t,\lambda,\mu)]$, que é função da densidade de probabilidade que o subsistema falhe no tempo "t" quando "s-1" reservas estão disponíveis e C=1;

3) $e^{-\mu t}$, que é a probabilidade de o "s-ésimo" reserva permanecer não-alimentado até o tempo "t", quando então isto é necessário;

4) $e^{-q\lambda(T-t)}$, que é a probabilidade de, após a "s-ésima" substituição, ocorrida no tempo "t", o sistema permanecer operando até o tempo T.

A solução para a equação recursiva apresentada é:

$$ {}_{c}R_{q}^{S}(T,\lambda,\mu) = e^{-q\lambda t} \sum_{k=0}^{S} \binom{k-1+q\frac{\lambda}{\mu}}{k} c^{k} (1 - e^{-\mu t}), $$

onde $\binom{k-1+q\frac{\lambda}{\mu}}{k}$ são coeficientes binomiais generalizados, desde que λ/μ não seja necessariamente inteiro.

h) Modelo por Markov

Os conceitos ligados a este método de modelamento são referentes a "estado" e "transição de estado". O "estado" de um sistema representa o que deve ser conhecido de forma a descrever este sistema em algum instante. A "transição de estado" está associada ao evento mudança de estado.

A consideração básica do modelo por Markov é que a probabilidade de uma dada transição de estado depende somente do estado atual. Para processos de Markov contínuos no tempo, o tempo já passado em um determinado estado não tem influência na distribuição da probabilidade do próximo estado e nem mesmo na distribuição da probabilidade de permanecer mais tempo neste mesmo estado. Esta consideração implica que, no caso contínuo no tempo, o tempo de espera gasto em cada estado é exponencialmente distribuído (Siewiorek, 1982).

Para sistemas com taxa de falhas e taxa de reparo constantes, os modelos de confiabilidade são associados a modelos de Markov contínuos no tempo. Estes modelos permitem as transições de estado ocorrerem aleatoriamente em intervalos variáveis, com taxas de transição associadas às possíveis transições. Estas taxas de transição, no caso da confiabilidade, são as taxas de falha e reparo, com a possibilidade de estas serem alteradas pelos fatores de chaveamento.

A modelagem por Markov é geral e pode ser aplicada a "sistemas fechados" e a "sistemas reparáveis". Estas são as duas categorias principais de computadores tolerantes a falhas. Sistemas fechados são aqueles que não permitem manutenção manual, por exemplo compu

tadores de veículos espaciais. Sistemas que permitem a manutenção manual no caso de falhas são chamados de sistemas reparáveis. Exemplos destes sistemas que permitem reparo são alguns tipos de processadores de chaveamento que possuem mecanismos de tolerância a falhas, tais como módulos reservas e a possibilidade de manutenção em caso de falha em algum módulo.

Alguns dos parâmetros associados ao modelo por Markov são:

N = número de módulos ativos;

S = número de módulos reservas;

λ = taxa de falhas de um módulo ativo;

ψ = taxa de falhas de um módulo reserva não-energizado;

μ = taxa de reparo de um módulo falho;

C = probabilidade de sucesso no chaveamento de um módulo ativo para um módulo reserva.

A Figura 2.8 mostra um exemplo de diagrama de estados por Markov:

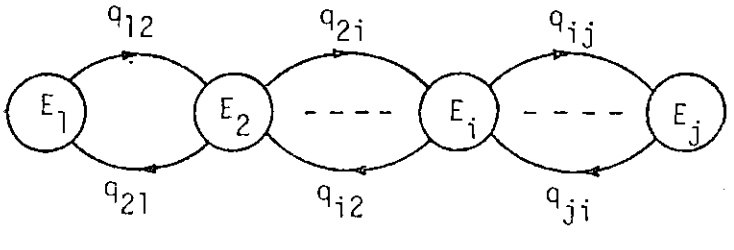


Fig. 2.8 - Diagrama de estados por Markov.

onde:

$Pi(t)$ = probabilidade do sistema estar, no tempo "t", no estado Ei;

$q_{ij}(t)$ = taxa, no tempo "t", com que o sistema parte do estado Ei para o estado Ej.

A transição para o estado seguinte depende somente do estado atual e não importa o passado. As taxas $q_{ij}(t)$ nos modelos de confiabilidade são associadas às taxas de falha e reparo.

A partir do diagrama de transição de estados mostrado na Figura 2.8 é obtida a matriz de taxa de transição de estados $\underline{A}$, que é dada por:

$$A = \begin{bmatrix} P_{11} & P_{12} \cdots\cdots P_{1j} \\ P_{21} & P_{22} \cdots\cdots P_{2j} \\ \vdots & \vdots \qquad \vdots \\ P_{i1} & P_{i2} \cdots\cdots P_{ij} \end{bmatrix},$$

onde P_{ij} = probabilidade de ocorrer uma transição para o estado "j" depois de um intervalo de tempo, dado que o sistema se encontra no estado "i" no início deste intervalo de tempo.

Dada à matriz $\underline{A}$, podem ser avaliadas as probabilidades limites do sistema se encontrar em cada estado através do sistema de equações dado por:

$$\underline{P} \cdot \underline{A} = \underline{P},$$

onde $\underline{P} = [P1\ P2\ \ldots\ Pi]$ e

Pi = probabilidade de o sistema estar no estado "i" (considerando $t \to \infty$).

O sistema $\underline{P} \cdot \underline{A} = \underline{P}$ significa que as probabilidades limites Pi para $t \to \infty$ não são afetadas quando multiplicadas pela matriz estocástica $\underline{A}$.

A disponibilidade A de um equipamento ou sistema é dada pela soma das probabilidades deste sistema se encontrar em um estado operacional, ou seja:

$$A = P1 + P2 + ... + Pn,$$

onde P1, P2, ... , Pn são probabilidades do sistema se encontrar em um estado operacional.

Outra maneira de obter a disponibilidade é

$$A = 1 - (Pn+1 + Pn+2 + ... + Pm),$$

onde Pn+1, Pn+2, ... , Pm são as probabilidade de o sistema se encontrar em um estado não-operacional, ou seja, de falha.

2.3 - TÉCNICAS UTILIZADAS PARA AUMENTAR A CONFIABILIDADE

Para aumentar a confiabilidade de um sistema, em particular os computadores de chaveamento em uma rede, diferentes técnicas podem ser utilizadas, sendo as mais importantes:

a) redução do número e complexidade dos componentes do sistema;

b) uso de componentes mais confiáveis;

c) uso de redundância;

d) uso de multiprocessadores ao invés de um único processador.

a) Redução do número de componentes

A taxa de ocorrência de falhas em um sistema sem redundância é a soma das taxas de falhas de cada componente que integra este sistema, considerando neste caso que a operação fora das especificações também é um estado de falha. Esta consideração é feita porque em alguns casos a falha em um componente pode levar o sistema não a uma falha imediata, mas a operar fora das especificações com falhas transitórias. Dado isto, torna-se clara a idéia de que diminuindo o número de componentes haverá um acréscimo no valor do MTBF (Tempo Médio Entre Falhas) e uma conseqüente melhoria na confiabilidade. O uso desta técnica pode implicar uma degradação na capacidade computacional de sistemas que operam em tempo real, pois isto é uma função direta do número de componentes. Dada esta limitação, pode ocorrer que o sistema execute tarefas em tempos mais longos que o previsto.

b) Componentes mais confiáveis

A confiabilidade de componentes pode ser melhorada com o uso de técnicas de fabricação mais sofisticadas, as quais envolvem testes de laboratório que simulam envelhecimento para que o componente supere a fase de "mortalidade infantil" (Siewiorek, 1982) e atinja a maturidade, além de outros testes. Mas, mesmo o uso de tais técnicas não consegue reduzir a taxa de ocorrência de falhas para o valor zero. O uso de componentes mais sofisticados gera dois problemas: componentes de alta confiabilidade custam caro e o simples uso deste recurso não descarta a necessidade de equipes de manutenção para executar o reparo em caso de falha de algum componente ou do sistema.

c) Redundância

Três formas de redundância podem ser utilizadas de maneira a contornar falhas:

- redundância temporal;

- redundância de programa;

- redundância de circuito.

A redundância temporal consiste em repetir periódicamente as operações da máquina ou segmentos de programa durante a sua fase de execução. Este procedimento auxilia a deteção de falhas que venham a ocorrer nesta fase.

A redundância de programas trata-se de rotinas básicas acrescidas aos programas básicos que se prestam a auxiliar na deteção de falhas e recuperação do sistema após a falha.

A redundância de circuito pode ser classificada em duas categorias: estática (mascaramento) ou dinâmica.

No caso do mascaramento, os componentes são utilizados de forma redundante de maneira a prover uma tolerância a falhas na qual o efeito de uma falha em um componente dentro do sistema não transparece para o meio onde se encontra tal sistema.

A redundância dinâmica é aplicada quando se deseja prover o sistema com a capacidade de deteção e recuperação imediata da falha, sendo que para isto necessita do auxílio de circuitos extras redundantes aos existentes (Anderson, 1981).

Um exemplo de redundância estática é o uso de códigos de correção de erros em memórias, enquanto um código de paridade pode ser encarado como uma redundância dinâmica, visto que este deteta o erro, mas necessita de redundância auxiliar para corrigir o erro. A redundância modular tripla (RMT) é tida como exemplo canônico de redundância estática. Em sua aplicação normal, a RMT é utilizada de maneira a prover tolerância em caso de falha em módulos de circuito ("hardware"). Assim, para tolerar uma falha em um módulo "R", pode-se substituir este módulo pelo sistema RMT, conforme mostra a Figura 2.9. A RMT consiste em três cópias idênticas ao módulo "R", mais o circuito de decisão

(votador) "V". Este circuito votador amostra as saídas dos três módulos e gera uma única saída igual a pelo menos duas das três que ele analisa, i.é., o votador mascara o erro quando uma das saídas se tornar diferente, e o sistema só vai falhar caso dois módulos falhem.

A utilização de unidades reservas pode ser considerada uma redundância dinâmica. Esta técnica consiste em utilizar módulos reservas nó sistema, de modo que tais módulos entrem em operação no caso de deteção de falhas nos módulos ativos. Desta maneira, o módulo avariado pode ser reparado sem que o sistema deixe de funcionar. Esta técnica aumenta bastante a disponibilidade do sistema, dado que é pequena a probabilidade de falha no módulo reserva, enquanto o módulo avariado está sendo reparado.

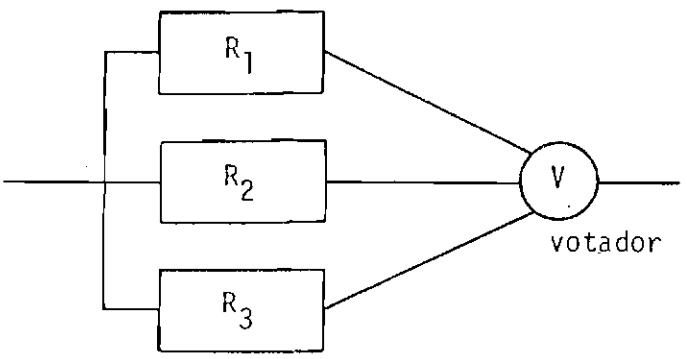


Fig. 2.9 - Redundância modular tripla.

A técnica de mascaramento, utilizada quando não há tempo para o reparo, tem seu custo muito elevado e por isto é utilizada em sistemas que exigem alta confiabilidade, como por exemplo lançadores ou controles de aeronave. A utilização de redundância dinâmica é mais aplicada em processadores de chaveamento em redes, dado que seu custo é menos elevado que o mascaramento.

d) Uso de multiprocessadores

O uso de multiprocessadores consiste em atribuir as tarefas do sistema a vários processadores e não a um único e poderoso processador. Nesta técnica, a memória principal é dividida em pequenos módulos que são gerenciados por cada processador. Os módulos constituídos pelas memórias e processadores são interligados de tal maneira que a falha em um dos módulos não provoque a queda do sistema, sendo possível a substituição do módulo defeituoso mesmo com o sistema em operação. A falha de um módulo tem como conseqüência apenas o decréscimo na capacidade computacional do sistema.

Em se tratando de processadores de chaveamento de uma rede de dados, as técnicas mais utilizadas para a melhoria da confiabilidade são o uso de multiprocessadores e a redundância dinâmica. O uso de multiprocessadores ocorre quando se necessita de uma grande capacidade computacional do sistema. Ambas as técnicas oferecem um custo aceitável e a disponibilidade mínima exigida para um processador de chaveamento.

2.4 - CONDIÇÕES QUE AFETAM A OPERAÇÃO DO PROCESSADOR DE CHAVEAMENTO

Problemas como erros, falhas, "deadlocks" e outros tantos afetam o desempenho de um processador de chaveamento e como conseqüência, diminuem a disponibilidade da rede (Makam, 1979). Os defeitos que podem alterar o comportamento dos processadores de comunicação são divididos em duas classes:

a) Falhas físicas: São causadas por falhas que ocorrem em um ou mais componentes que integram o sistema. Tais falhas podem ter como conseqüência uma mudança temporária no comportamento lógico do sistema, resultando em erros ou numa parada permanente nas funções computacionais.

b) Falhas humanas: São causadas por imperfeições no projeto, tanto na área de "hardware" como na área de "software", e por ações inadequadas dos operadores. Os efeitos são similares aos causados pelas falhas físicas.

Com relação à rede de computadores ainda existem problemas que lhes são particulares:

a) Ruído no canal de comunicação: É causado por interferências atmosféricas. Os efeitos são erros de "burst" que afetam blocos de dados que estão na linha de transmissão.

b) Erros em componentes de comunicação: Se intermitentes, causam perdas de dados nos nós receptores, se permanentes, causam a perda de conexão entre nós.

c) Protocolos incorretos ou incompletos: Os protocolos estabelecem certas regras para que seja mantida corretamente uma comunicação. Os problemas relativos à implantação de protocolos incorretos ou imcompletos são:

- perda de sincronização na comunicação, o que causa atrasos e perdas de dados;
- "deadlocks";
- ineficiência no estabelecimento de conexões.

d) "Deadlocks" e "lock-up" na rede: Estes problemas existem devido à limitação de recursos ("buffers") e rotinas de roteamento e controle de fluxo inadequadas. A ocorrência de "lock-up" implica que nada pode ser processado na parte da rede que foi afetada por este problema. O "lock-up" ocorre devido à falta de "buffers" suficientes nos nós, o que impossibilita o fluxo correto de dados na rede. O efeito imediato é o congestionamento na rede, que resulta em atrasos excessivos e perda de sincronismo entre processos.

2.5 - EXEMPLOS DE PROCESSADORES DE CHAVEAMENTO COM TOLERÂNCIA A FALHA

Os processadores de chaveamento, descritos a seguir, empregam diversas técnicas de maneira a tornar o sistema mais confiável. A análise destes equipamentos permite tomar conhecimento da aplicação prática de tais técnicas, bem como analisar os resultados e melhorias obtidas. A ênfase dada nestas análises diz respeito aos mecanismos utilizados no "circuito" ("hardware") de cada um destes equipamentos.

2.5.1 - PROCESSADOR DE COMUNICAÇÃO TELENET-TP4000

O equipamento TP-4000 é um processador de comunicação baseado na utilização de multimicros, i.é., possui vários micros operando em conjunto, cada um responsável por uma tarefa, que pode ser o gerenciamento de uma linha serial ou processamento em geral (TELENET, 1977).

A estrutura do TP-4000 é descrita na Figura 2.10 (TELENET, 1977).

A modularidade do sistema permite que ele seja configurado de uma maneira redundante ou não-redundante.

O sistema possui duas CPUs, dois barramentos internos, dois bancos de memória, dois árbitros, etc. Desta maneira, o sistema procura prover todo tipo de redundância de modo que uma falha simples não cause a queda nas comunicações.

O sistema TP-4000 possui processadores dedicados ao controle de linhas seriais (LPUs). Os LPUs são configurados de maneira a gerenciar 4 linhas assíncronas ou 8 linhas síncronas, ou 4 linhas com sincronismo binário ou 8 linhas SDLC. Os LPUs operam independentemente da CPU e da memória principal, mas como se trata de um sistena de multiprocessamento, os LPUs recebem controles da CPU, os quais podem colocá-los em estado de "espera", "execução", ou "execução passo a passo".

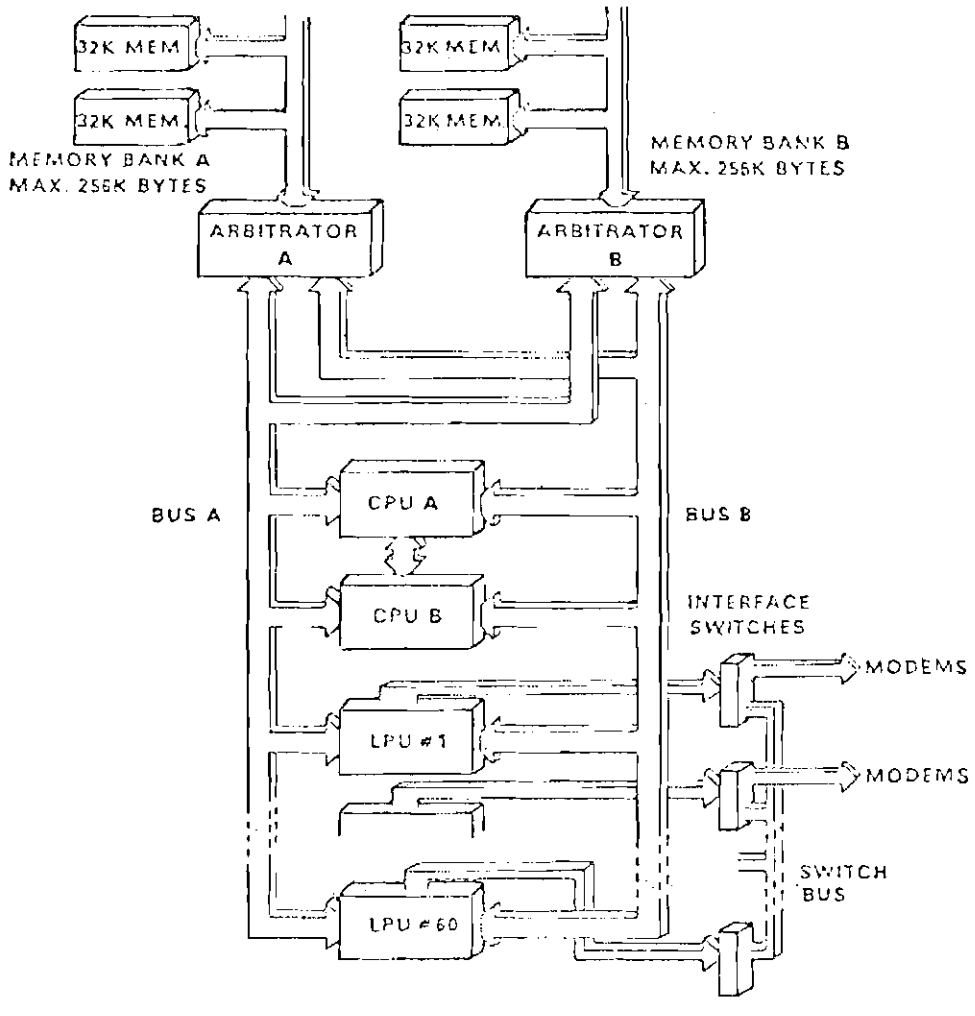


Fig. 2.10 - Estrutura do equipamento TP 4000.
FONTE: Opderbeck, 1978, p.4

As CPUs são em número de dois e operam independentemente uma da outra, ou no modo reserva. Operando com uma unidade reserva há uma alta confiabilidade, enquanto operando independentemente uma da outra, obtém-se o dobro de capacidade de processamento. As CPUs, além de estarem ligadas aos barramentos internos ao sistema, possuem uma conexão entre si chamada "INTRA CPU LINK", através da qual são trocadas informações de "status" diretamente. No caso de uma CPU estar na condição de ativa e outra na condição de reserva, é através deste barramento que é feita a transferência de dados da CPU ativa para a CPU reserva, em caso de falha da CPU ativa, pois a CPU reserva deve adaptar a condição de ativa.

Existem dois barramentos no sistema, aos quais estão conectadas as CPUs, os LPUs e os árbitros que controlam o acesso aos bancos de memória. Este tipo de ligação garante uma redundância no acesso às memórias.

Os bancos de memória possuem até 8 módulos de 32 K"bytes" cada um, perfazendo um total de no máximo 256 K"bytes" em cada banco de memória e 512 K"bytes" considerando os dois bancos de memória. Existe verificação de paridade nos bits de endereço e bits de dados na memória. Estas memórias são utilizadas pelos LPUs e pelas CPUs para realizar transferência de mensagens entre processadores, ou somente para armazená-las.

Os árbitros controlam o acesso aos bancos de memória e têm a capacidade de verificação cíclica de erros de paridade nas memórias. Da mesma forma, todas as informações que passam através dos barramentos da memória principal para os LPUs e CPUs são monitoradas pelos árbitros com respeito a erro de paridade.

Tanto as CPUs como os L s possuem memórias locais; a CPU possui 16K (de um total de 64K) de memória local e o LPU possui 8K (de um total de 64K). O restante, tanto da CPU como do LPU, se encontra na memória principal (banco de memórias). A CPU pode ter mais 1K de PROM de modo a ter "software" básico para a interface TTY.

Todos LPUs são ligados às linhas através de interfaces especiais que são conectadas entre si. Em caso de falha em um LPU, as linhas ligadas a este LPU são chaveadas para outro LPU reserva, automaticamente.

O sistema possui duas fontes que operam independentemente e que são acopladas através de diodos. Isto garante que a falha em uma fonte não afeta a operação da outra fonte.

Tanto a CPU como o LPU utilizam o mésmo tipo de processador de 8 bits, o CI 6502-A de tecnologia MOS.

Um temporizador, que funciona como "cão de guarda", atua na CPU e no LPU e verifica periodicamente o funcionamento do "hardware" e do "software".

Caso ocorra erro de paridade quando a CPU ou o LPU acessam a memória principal, ambos possuem a capacidade de realizar este acesso novamente por um certo número de vezes. Se as tentativas não tiverem sucesso, um sinal é acionado e uma interrupção é gerada ("restart"), indicando o erro.

O "software" do TP-4000 está baseado no protocolo de interfaceamento X.25. Este protocolo é utilizado de duas maneiras diferentes:

1) como uma interface comum para conectar o TP a uma rede;

2) como uma interface interna para operar uma rede formada por TPs (Opderbeck, 1978).

Para pequenas redes formadas por TPs é utilizado um equipamento adicional para prover rotinas de roteamento, endereçamento e tabelas para estes fins, o qual é denominado Centro de Controle da Rede (CCR).

2.5.2 - SISTEMA DE MULTIPROCESSADORES TANDEM 16

O sistema TANDEM 16 foi projetado para obter alta disponibilidade em aplicações do tipo "on-line". A filosofia básica deste equipamento é aquela que afirma que uma falha simples não deve causar interrupção no serviço e que em caso de falha haja condição de reparo sem afetar o resto do sistema. A manutenção "on-line" foi um fator chave por ocasião do projeto das placas de circuito bem como da distribuição das fontes de energia do sistema (Katzman, 1977).

Para que os objetivos expostos sejam alcançados o "hardware" utilizado é duplicado em vários pontos (fontes, barramentos, controladores, etc.), e o "software" também é dotado de redundância ao nível de processo. O esquema utilizado é o de multiprocessadores; a configuração mínima do sistema TANDEM 16 é a de 2 processadores, e a máxima é de 16 processadores. A Figura 2.11 ilustra a arquitetura do sistema TANDEM 16 (Katzman, 1977).

O sistema TANDEM 16, opera com vários módulos processadores (mínimo 2 e máximo 16) que se comunicam entre si através de um sistema de barramentos denominado DYNABUS. O DYNABUS é composto de dois barramentos idênticos, o que significa uma redundância total no barramento entre processadores.

Os módulos processadores são compostos de três partes principais: CPU, memória e canal de I/O (Figura 2.11).

A CPU é um processador microprogramado composto de dois estágios conectados no esquema "pipeline". A memória é dividida em blocos de 1K, com palavras de 16 bits e possui dois tipos de deteção de erros: um no sistema de memória semicondutora, onde há 6 bits/palavra que servem para verificação de erro, realizando correção em erro simples e deteção de erro duplo, e outro tipo no sistema de memória central, onde um bit de paridade é utilizado para detetar erro simples.

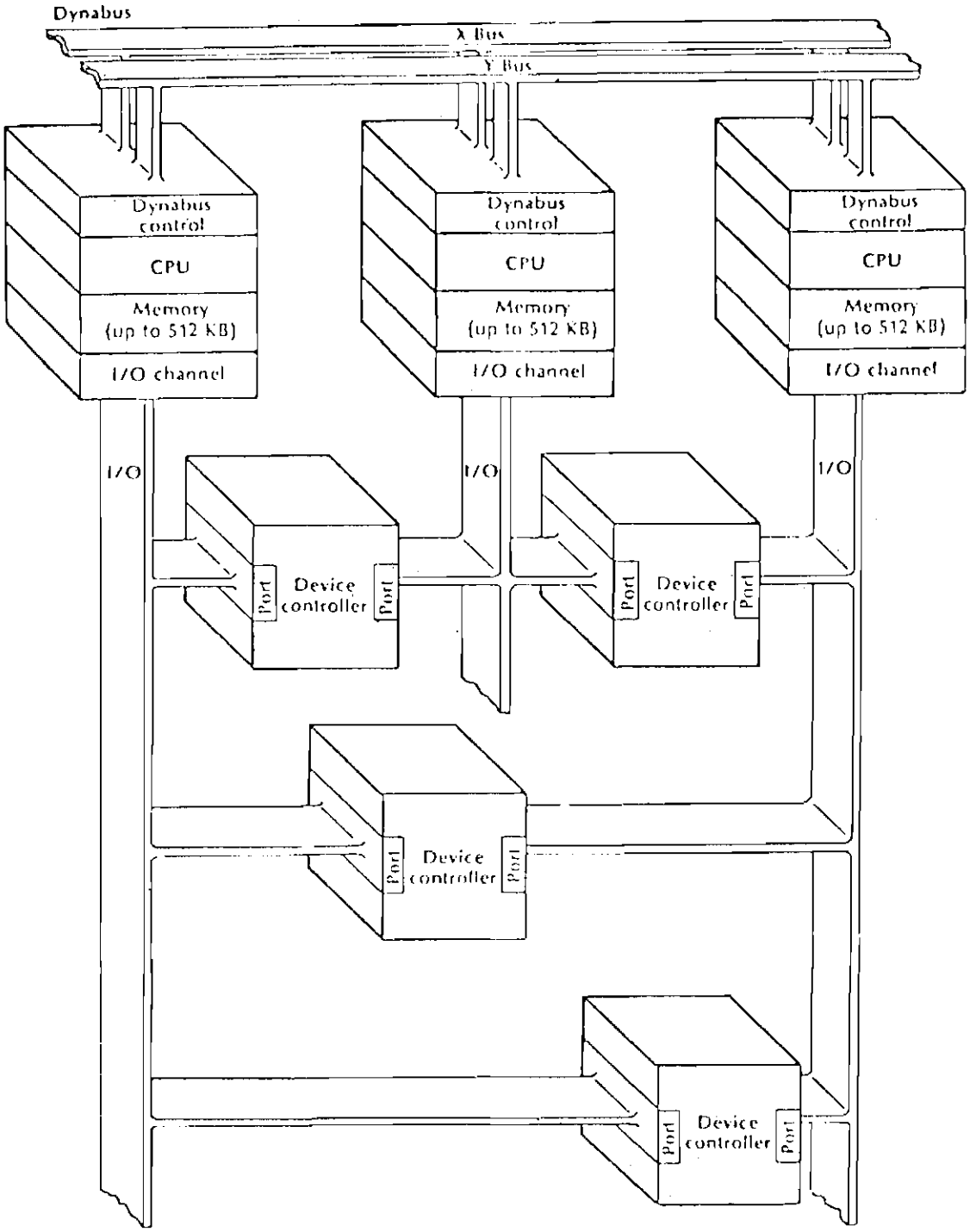


Fig. 2.11 - Arquitetura do Sistema TANDEM 16.
FONTE: Katzman, 1977, p.437.

A transferência de mensagens entre processadores é feita através do DYNABUS, sendo que o controle é realizado pelo "hardware" e os dados são transferidos diretamente de memória para memória. O esquema utilizado para a transferência é o de "pacotes". Cada "pacote" é composto de 15 palavras e 1 palavra de verificação. A cada "pacote" transmitido o processador fonte sinaliza um temporizador, o qual, caso a transferência não seja concluída dentro do intervalo de tempo previsto, aciona um mecanismo de retransmissão. Este modo de transmissão caracteriza total isolamento entre os processadores, visto que eles não usam um equipamento em comum para realizar a transferência de dados, como por exemplo uma memória compartilhada.

Os canais de I/O operam através de DMA e consistem em um barramento com 2 "bytes" de dados e sinais de controle. Todos os dados que passam por este barramento de I/O têm verificação de paridade e os erros informados através de interrupção. Cada canal de I/O é conectado a controladores de I/O que têm a função de prover a interface adequada entre o canal de I/O padrão do TANDEM 16 e uma variedade de periféricos, utilizando interfaces distintas. Cada controlador de I/O é dotado de duas vias de acesso, e cada via de acesso, ou porta, está conectada a um canal de I/O diferente (Figura 2.11). Para permitir a redundância, um canal de I/O deve ser ligado a dois controladores de I/O, os quais estão ligados a um mesmo periférico. Desta maneira, caso um controlador falhe, o outro assume o papel de ativo, permitindo o acesso ao periférico.

Como os controladores de I/O são conectados entre dois canais de I/O distintos, é importante que cada canal armazene as informações utilizadas para comandar o controlador, pois em caso de falha neste controlador não há perigo de queda nos canais ligados a ele.

Cada módulo processador possui sua própria fonte, sendo que cada controlador de I/O é alimentado por duas fontes independentes, conectadas juntas através de um esquema de diodos, o que garante um suprimento contínuo de energia no caso de falha de uma das fontes. O esquema de alimentação descrito é mostrado na Figura 2.12 (Katzman; 1977).

Assim como o "hardware", o "software" do sistema TANDEM 16 é baseado na idéia de utilizar redundância como uma maneira de tolerar falhas simples. O uso de tal redundância também visa aproveitar a redundância já existente no "hardware".

O sistema operacional do TANDEM 16, também chamado "GUARDIAN", utiliza o conceito de processos e mensagens. Os processos que são responsáveis por acesso a dispositivos de I/O são implementados em pares, sendo que um é atuante (primário) e o outro reserva.

O processo primário envia constantemente informações de "status" ao processo reserva. Deste modo, o processo reserva pode ter a condição de primário em caso de falha deste.

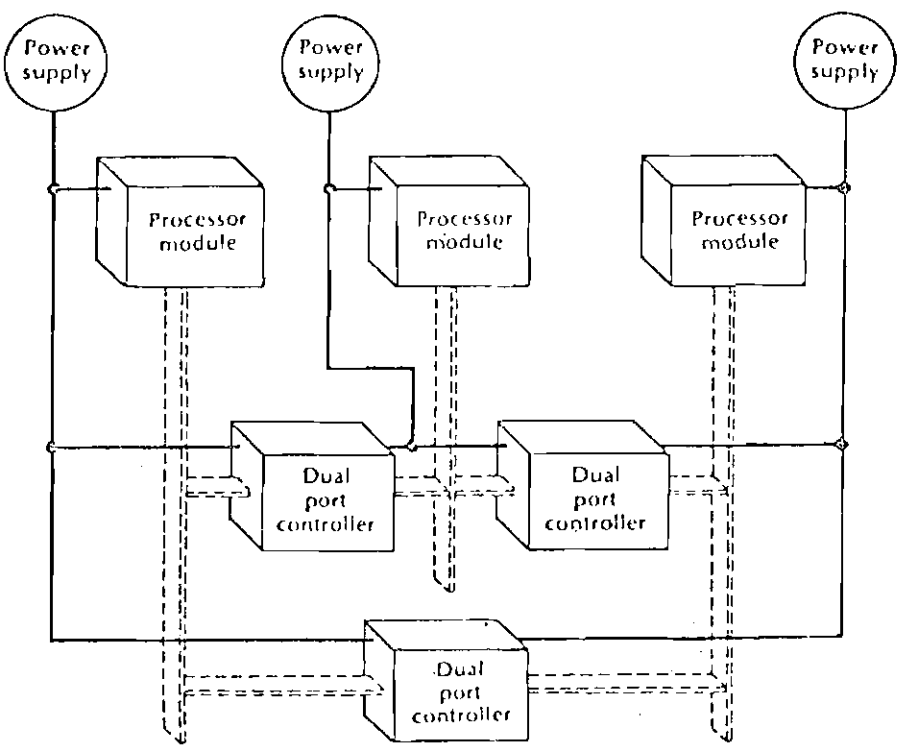


Fig. 2.12 - Esquema de alimentação do Sistema TANDEM 16.
FONTE: Katzman, 1977, p.438.

2.5.3 - PROCESSADOR ESS-3A - BELL SYSTEM

Os processadores ESS (Electronic Switching Systems) dos Laboratórios Bell (USA) foram desenvolvidos para prover um serviço telefônico adequado, cuja taxa de falhas seja a mínima possível. Foram desenvolvidas varias versões do processador ESS, cada uma habilitada a atender uma certa quantidade de usuários (Toy, 1978).

O processador do qual é feita uma análise é o ESS-3A, que é de pequeno porte e atende de 500 a 5000 linhas. Os outros tipos de processadores ESS existentes são: ESS-1 e ESS-2, estes dois de primeira geração, e ESS-1A e ESS-2A de segunda geração, originada com o advento da integração dos componentes eletrônicos. Estes processadores têm capacidade maior que o ESS-3A.

Uma das maiores vantagens do ESS-3A é o seu baixo custo e a alta velecidade de seu processador, o que garante um desempenho melhor que a de seu predecessor, o ESS-2.

O ESS-3A utiliza técnica de microprogramação em seu processador central, e como o número de componentes neste sistema é consideravelmente menor que os outros processadores ESS, todos os sub-sistemas são inteiramente duplicados, incluindo a memória principal.

O projeto do ESS-3A possui uma diferença fundamental dos ESS anteriores, pois este sistema opera com circuitos redundantes sem realizar comparação entre os resultados obtidos pelas duas unidades redundantes. O objetivo principal da comparação é detetar erros. Entretanto, a comparação apesar de detetar a falha não indica onde ela ocorreu, pois para isto é necessário o auxílio de um "software" adicional, de maneira a encontrar o defeito e desconectar a unidade defeituosa. Sem o uso da comparação, um sistema opera normalmente e o outro fica em reserva, sendo que para detetar o erro o ESS-3A é provido de um "hardware" que realiza autoverificação incorporada ao processador.

A Figura 2.13 ilustra a arquitetura utilizada no processador ESS-3A (Toy, 1978).

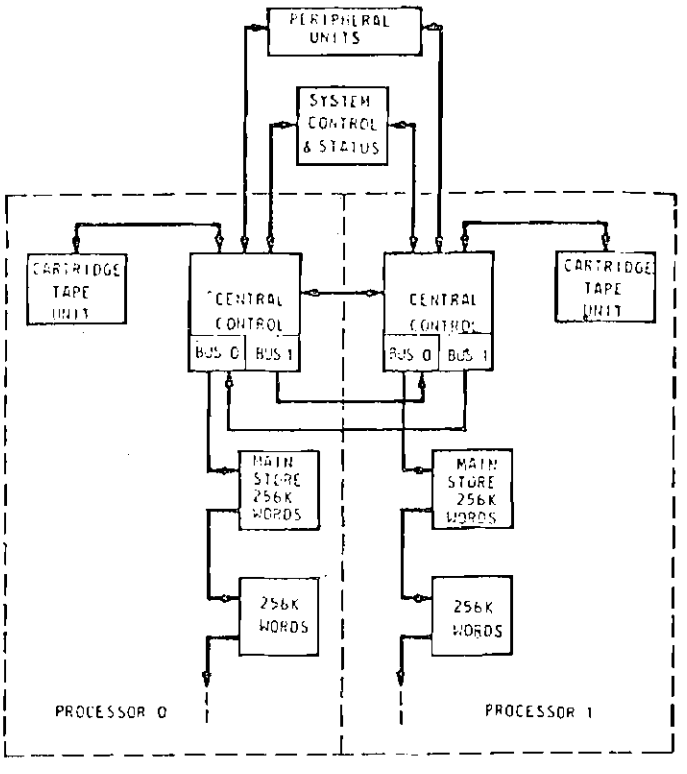


Fig. 2.13 - Arquitetura do Processador ESS-3A.
FONTE: Toy, 1978, p.1134.

Dois processadores são utilizados, sendo que em operação normal o processador ativo ("on-line") é responsável por "rodar" e processar as chamadas, enquanto o reserva fica no estado "parado". A operação de escrita atua sobre as memórias dos dois processadores, visando manter a memória da unidade reserva atualizada. Durante o processo de leitura, o acesso é permitido somente à memória da unidade ativa, exceto quando um erro de paridade ocorre durante a leitura, o que resulta numa interrupção no microprograma, o qual lê a palavra da memória reserva de modo a deixar o erro transparente ao meio externo.

Por causa da natureza volátil da memória, onde se realiza a escrita, é necessário um equipamento para armazenamento de dados de maneira a recarregar os programas e dados em geral quando estes são perdidos devido à falha de armazenamento na memória. É interessante que tal equipamento seja de baixo custo, pois teria o papel de uma redundância extra. São utilizadas fitas cartucho para este fim.

O ESS-3A possui 20 canais principais de I/O, cada um com 20 subcanais, o que permite ao processador o controle e acesso a até 400 unidades de periféricos.

O fato de o circuito operar com processador microprogramado permite que as técnicas de deteção de erro tenham uma ação mais rápida, visto que a microinstrução é a operação mais elementar na máquina. Microinstruções possuem dois tipos de dados: códigos de controle e informações sobre endereços.

No ESS-3A as informações de controle (dois campos com 8 bits) são codificadas utilizando o código 4-de-8 (m-de-2m), o qual permite um máximo de detetabilidade a um custo mínimo. Este código pode detetar todos os erros unidirecionais múltiplos. Erros unidirecionais referem-se a falhas que fazem com que bits de dados assumam valores errôneos de um único tipo = 0 ou 1, mas não os dois simultaneamente (por exemplo 01100 para 01111, e não para 01010). Todas as palavras deste código contêm exatamente 4 bits iguais a 1 e, usando palavra de 8 bits, existem 70 palavras possíveis de ser usadas.

As informações de endereço que fazem parte da microinstrução são codificadas por um bit de verificação de paridade simples. Os bits do endereço são entrelaçados com os bits de controle, a fim de permitir a deteção de qualquer erro de 2 bits consecutivos.

Os processadores possuem 16 registros de uso geral, e os dados nestes registros, bem como na memória principal, são codificados utilizando dois bits de paridade. A verificação é feita a cada transferência de dados de uma posição para outra no processador.

A unidade central de controle é verificada periodicamente por dois temporizadores que funcionam como "cães de guarda". Desta maneira, se um "time-out" ocorre, um erro é detetado e o sistema inicia o procedimento de recuperação.

No ESS-3A a recuperação pode ser automática ou manual. A recuperação automática tem início assim que um erro é reconhecido pelo processador ativo. Os sinais de erro são armazenados no registro de erros (RE) para que possa ser feita uma diagnose posterior. Além disto, os sinais de erro são ordenados divididos em três grupos, cada um causando um conjunto de ações diferentes por parte dos sistemas.

O menos grave destes três grupos de erros é o grupo de erros associado aos dispositivos de I/O. Este tipo de erro causa uma interrupção pela qual o processador possui um controle completo de maneira a determinar a causa exata do problema. Se o erro é uma falha transiente, a informação sobre este erro é armazenada para uma análise posterior. Caso o erro seja devido a uma falha de "hardware" dentro de um dos blocos que compõe o processador, então o programa que atende à interrupção inicia uma reconfiguração, chaveando para unidade reserva através do canal especial de manutenção.

O segundo tipo de erro envolve falhas que ocorrem na unidade reserva do sistema. Estas falhas influenciam diretamente na operação da unidade ativa. Por exemplo, o procedimento de escrita em memória é feito tanto na memória ativa como na memória reserva e ambas enviam sinal de confirmação para o processador proceder a próxima operação. Se a resposta for gerada apenas pela memória ativa, um certo período de tempo é esperado para a chegada da resposta da memória reserva e, se este sinal não chega dentro deste período, um circuito especial de "time-out" gera um sinal de erro que indica o problema. Uma interrupção é gerada e o processador continua na operação normal, mantendo isolada a unidade com defeito.

O terceiro tipo de erro envolve falha no "hardware" do sistema ativo. Para ilustrar este tipo de erro basta retomar o exemplo do acesso às memórias do sistema. Se o sinal de confirmação de escrita é recebido da unidade reserva e não da unidade ativa, é gerado um sinal de erro que força o chaveamento do sistema para a unidade reserva. Nesta situação o sistema sai do ar momentaneamente e um sinal de inicialização ("restart") na unidade reserva inicializa seu processador, o qual continua o processo de chamadas, afetando talvez apenas a chamada que estava sendo processada durante o estado de transição.

A recuperação manual é necessária quando o sistema não é capaz de recuperar-se através do procedimento automático. Isto pode ocorrer devido à falha no "software" ou no "hardware" de deteção, ou em ambos.

2.5.4 - PLURIBUS

O PLURIBUS é um processador de chaveamento utilizado na rede ARPA (EUA). Seu projeto foi motivado devido à necessidade da expansão da rede ARPA, com conseqüente acréscimo no número de hospedeiros, volume de tráfego e área geográfica a ser coberta. O objetivo estabelecido para o projeto foi a obtenção de uma máquina modular, capaz de servir um número maior 5 vezes de equipamentos de entrada/saída, com uma memória maior e mais confiável (Katsuki, 1978).

A arquitetura utilizada foi o uso de multiprocessadores para obter a modularidade, baixo custo para alto desempenho e confiabilidade. Desta maneira os algoritmos residentes no nó (processador de chaveamento) podem ser executados paralelamente e por processadores diferentes.

O PLURIBUS se comunica com computadores hospedeiros e com terminais assíncronos. As funções de um PLURIBUS são de um processador de comunicação, implementado para isto rotinas de roteamento de mensagens, controle de fluxo de mensagens, controle de erro, armazenamento temporário de mensagens, divisão e seqüenciamento da mensagem em

em pacotes, montagem da mensagem a ser entregue e monitoração de "status" de hospedeiros e linhas.

O meio em que o PLURIBUS opera (rede de comunicação de dados) permite que seja aceitável a perda ocasional de algumas mensagens ou breve parada na operação, visto que diante de uma destas falhas os níveis mais altos do protocolo de comunicação que opera na rede se encarregam de realizar a retransmissão dos dados, se necessário. Este equipamento opera 24 horas por dia e muitas vezes em locais sem acesso imediato, o que mostra a necessidade de uma arquitetura confiável e tolerante a certos tipos de falhas, para que a recuperação ocorra em poucos segundos.

O "hardware" do PLURIBUS é baseado em uma estrutura modular com três módulos básicos:

- modulo processador (processor bus),
- módulo memória (memory bus),
- módulo E/S (I/O bus).

A estrutura de cada um destes módulos é mostrada na Figura 2.14 (Katsuki, 1978).

Cada módulo tem seu próprio sistema de ventilação e sua própria fonte.

O sistema utiliza o minicomputador Lockeed SUE de 16 bits (similar ao DEC PDP 11). Esta máquina incorpora uma estrutura de endereçamento unificada e um barramento assíncrono, multiplexado no tempo. Isto permite grande facilidade na combinação de processadores, memórias e unidades de entrada e saída. A lógica que controla o barramento é separada fisicamente do processador SUE. Esta característica permite ao barramento ter um ou vários processadores, ou nenhum. O PLURIBUS utiliza o barramento, a lógica de controle do barramento, processadores, memória e várias unidades de E/S do SUE.

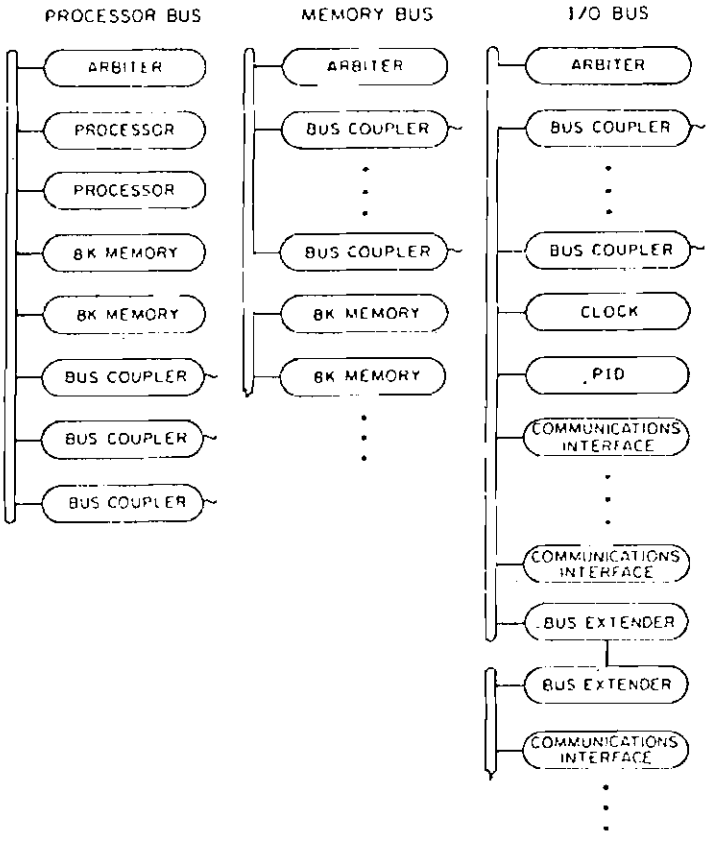


Fig. 2.14 - Estrutura dos módulos do Sistema PLURIBUS
FONTE: Katsuki, 1978, p.1149.

- *Módulo processador:* Contém um ou dois processadores, memória local, árbitro de barramento e um acoplador de barramento (lógico). Na aplicação corrente são necessários de 8K a 12K de memória local para cada processador (Figura 2.14).

- *Módulo memória:* Contém um árbitro, acoplador de barramento (lógico) para outras placas e memórias o bastante para suportar a aplicação. O sistema pode ter até 512K de memória, entretanto este montante de memória não se encontra em um único módulo memória. Sistemas típicos do PLURIBUS têm de 32K a 80K de memória em cada módulo, dependendo da aplicação (Figura 2.14).

- *Módulo E/S:* Possui, além do árbitro de barramento e do acoplador de barramento (lógico), placas para vários tipos de "interfaces" de E/S requeridos, incluindo "interface" para MODEMS, terminais, computadores hospedeiros, etc., bem como para periféricos comuns (Figura 2.14). Este módulo tem duas unidades especiais:
  - um relógio de tempo real (RTC), o qual é utilizado pelo sistema para temporizar processos e elos ("links") de comunicação.
  - dispositivo de pseudo-interrupção (PID), circuito auxiliar no qual os eventos escrevem o valor da prioridade da interrupção que seria gerada com a sua ocorrência.

A conexão entre módulos é feita através de uma placa chamada "acoplador de barramento". Para conectar os processadores à memória comum do sistema, uma placa "acoplador de barramento" é instalada no módulo memória e outra no módulo processador. A conexão é similar entre cada módulo processador e cada módulo E/S. Desta maneira, todos processadores podem acessar a memória comum e qualquer unidade de E/S.

Dispositivos de E/S, que se utilizam do mecanismo de ADM, têm em seu módulo placas "acopladores de barramento" ligadas diretamente aos módulos de memória.

A placa "acoplador de barramento" do módulo memória e do módulo E/S possui circuitos de reconhecimento que podem ser programados através de "jump's", os quais selecionam uma certa faixa de endereços que dá acesso ao barramento destes módulos. Desta forma, quando os processadores fazem referência a barramentos comuns à memória e aos dispositivos de E/S, e é gerado um endereço, os circuitos de reconhecimentos (que não passam de decodificadores) permitem acesso somente ao barramento que realmente deve ser consultado (memória ou E/S) para requerer um ciclo de serviço. Isto faz com que o barramento que não deve ser consultado não seja contido desnecessariamente para um ciclo de serviço.

Os módulos processadores têm acesso a outros módulos processadores através de placas "acoplador de barramento" ligadas aos módulos E/S. Esta comunicação é necessária para disparar ou parar outros processadores ou recarregar suas memórias.

A inserção ou a remoção de módulos processadores é permitida, pois os caminhos que os ligam à memória e aos dispositivos de E/S (placas "acoplador de barramento") têm chaves de habilitação programadas por "software". Normalmente a comunicação com a memória e dispositivos de E/S está habilitada. O caminho inverso é liberado mediante uma senha gerada pelo processador. Um processador não pode habilitar/desabilitar o acesso a si próprio, mas um processador pode decidir que outro está operando em estado anormal (falho) e retirá-lo do barramento.

A deteção de erros nos barramentos de acoplamento é feita através de código de paridade, usando deteção do tipo "todos bits em 1" ou "todos bits em zero". Este tipo de deteção é aplicado em todas as comunicações entre os módulos.

No PLIRUBUS existe no mínimo um módulo extra de cada tipo (processador, memória e dispositivos de E/S). Os recursos redundantes não ficam inoperantes, e são utilizados para incrementar o desempenho do sistema. As "interfaces" de E/S são duplicadas em diferentes módulos E/S, mas ambas ligadas a um único cabo (não-redundante) que sai da máquina. O que existe são duas "interfaces" ligadas a um mesmo cabo, e isto é possível porque uma delas fica em estado de alta impedância, saindo deste estado somente se a "interface" de E/S que está operando falhar.

Cada "interface" de E/S tem um temporizador "cão de guarda", e se esta "interface" não responde ao acesso do processador dentro de um certo tempo estabelecido, ela é desconectada.

Manter a confiabilidade do sistema é tarefa do "software" que tem como funções:

- "rodar" o programa de testes periodicamente;

- reconfigurar o sistema utilizando os módulos redundantes existentes:

- verificar a validade das estruturas de dados utilizando também a informação redundante;

- recuperar o sistema em caso de falha não detetada em tempo útil.

A manutenção da confiabilidade do PLURUBUS requer o conhecimento dos recursos disponíveis de "hardware" e "software". Um mapeamento de todo o sistema é feito pelo "software" passo a passo, sendo que cada passo depende do passo anterior ter tido sucesso. Sob este ponto de vista, os programas aplicativos só "rodam" depois de testados todos os elementos ("hardware" e "software") do sistema.

2.5.5 - CENTRAL DE COMUTAÇÃO DE PACOTES - CCP/USP

A Central de Comutação de Pacotes (CCP) é uma central experimental desenvolvida em conformidade com os requisitos básicos para sua utilização numa rede de computadores. O projeto foi desenvolvido no Laboratório de Sistemas Digitais da EPUSP, com o objetivo de proporcionar a partilhamento eficaz de recursos computacionais e a formação de recursos humanos na área de redes de computadores.

A central se baseia na aplicação de uma máquina de arquitetura distribuída que envolve o uso múltiplo de microprocessadores. A estrutura lógica e física da central obedece aos princípios básicos de sistemas concorrentes e distribuídos: processos concorrentes, comunicação através de mensagens, capacidade de reconfiguração, etc. (Barbosa, 1982).

A CCP tem as seguintes funções:

1) tratamento do protocolo X.25 com os computadores hospedeiros e outras CCPs;

2) definição das rotas e encaminhamentos de mensagens;

3) comunicação com unidades de armazenamento e impressão;

4) comunicação com o operador;

5) coleta de estatísticas.

A CCP é uma máquina de arquitetura distribuída sob o ponto de vista lógico. Para implementá-la é utilizado um conjunto de processadores com capacidade de armazenamento local, interligados por um sistema de comunicações.

Os elementos com capacidade de processamento e armazenamento local são chamados Processadores Monolíticos (PM) e são interligados através de um Sistema de Interconexão (SI), conforme mostra a Figura 2.15 (Barbosa, 1982).

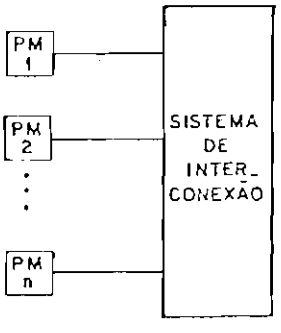


Fig. 2.15 - Sistema de interconexão - CCP/USP.
FONTE: Barbosa, 1982, p.76.

A estrutura interna do PM é mostrada na Figura 2.16.

O PM é conectado ao SI através de uma Interface de Comunicação (IC). Esta interface é responsável pela transmissão e recepção de mensagens enviadas ou recebidas pelo PM. Um PM pode possuir um ou mais ICs.

O SI fornece o meio físico necessário à interligação dos PMs e, para isto, utiliza um esquema de chaveamento indireto que envolve a comutação de mensagens. O SI é composto pela coleção de ICs interligados em um esquema de anéis duplos, conforme é mostrado na Figura 2.17.

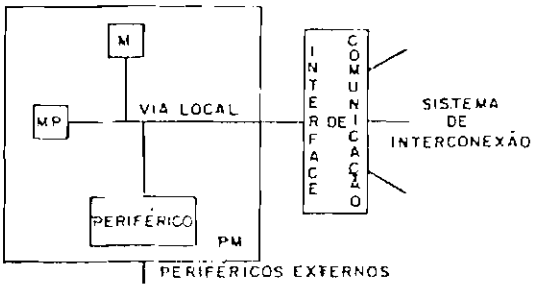


Fig. 2.16 - Estrutura interna do PM - CCP/USP.
FONTE: Barbosa, 1982, p.76.

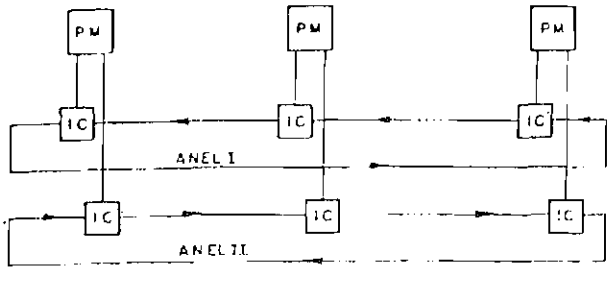


Fig. 2.17 - Estrutura do sistema de interconexão - CCP/USP.
FONTE: Barbosa, 1982, p.77.

Além da interface do PM com o SI, as ICs são responsáveis também pelo procedimento de encaminhamento de mensagens e pela execução dos protocolos internos ao SI.

Para a execução de tarefas na CCP, é alocado um conjunto de PMs, sendo que cada PM é responsável pela execução de um conjunto de processos. Este mapeamento possui uma característica dinâmica, ou seja, é possível alterá-lo durante o processamento. A possibilidade de um mapeamento dinâmico é o elemento fundamental para dotar a máquina de capacidade de reconfiguração. Toda vez que for detetada a falha em um PM, o que é feito através dos circuitos existentes detetores de falhas, deve ser ativado um processo reconfigurador que isola o elemento em falha e realoca o conjunto de processos associados ao PM que falhou a um outro PM disponível.

A interface do PM com o anel de comunicação é mostrada na Figura 2.18.

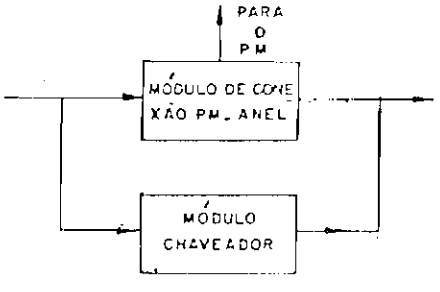


Fig. 2.18 - Configuração da interface do anel de comunicação -CCP/USP.
FONTE: Barbosa, 1982, p.77.

Na Figura 2.18 tem-se:

- *Módulo de conexão PM-anel:* responsável pela transmissão e recepção de mensagens do PM para o anel, incluindo armazenamento temporário de mensagens recebidas, transmitidas e em trânsito pelo anel, inserção no anel de mensagens transmitidas pelo PM, deco

dificação do campo de endereços de mensagens recebidas, deteção de erros de transmissão, deteção de falhas e desativação da interface do anel imediatamente anterior;

- *Módulo chaveador:* responsável pela desconexão do módulo de conexão PM-anel, quando este falhar, e pelo fechamento do caminho no anel neste ponto.

Internamente um PM é formado por dois tipos de módulos: módulo básico e módulos de expansão. Estes módulos são interligados através de uma via de comunicação interna conforme mostra a Figura 2.19.

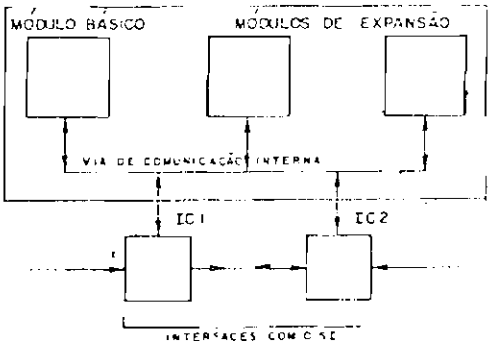


Fig. 2.19 - Via de comunicação interna - CCP/USP.
FONTE: Barbosa, 1982, p.77.

O módulo básico é comum a todos os PMs. Possui os "circuitos" ("hardware") necessários para a conexão com o SI e a execução dos programas necessários para a depuração, controle e comunicação, além de circuitos utilizados para deteção de falhas, como temporizadores para programas e geradores/testadores de paridade para a via de dados.

Um circuito desativador desativa o PM quando ocorrer um erro de paridade na via de dados ou quando for detetada uma falha por temporização.

A via de comunicação interna pode ser dividida em três grupos de sinais:

- sinais de endereço (16 bits);

- sinais de dados (8 bits + 1 bit de paridade);

- sinais de controle para operação dos demais blocos.

Os módulos de expansão que compõem o PM são divididos em dois tipos:

Módulos de entrada/saída: Contêm os circuitos adicionais específicos para comunicação com dispositivos externos, (linhas de transmissão, terminais, impressoras, discos, etc.).

Módulos de expansão de memória: Contêm somente memória.

A arquitetura física da CCP é composta de pelo menos 4 PMs dedicados exclusivamente ao processamento de pacotes (PMP) e 9 PMs dedicados ao processamento de operação de entrada e saída (PMD). Todos os PMs estão conectados ao SI que possui uma estrutura de anéis duplos circulando em sentidos opostos.

2.5.6 - CONCLUSÃO

Os sistemas apresentados têm em comum a natureza de operação em que estão envolvidos que é a de processadores de chaveamento (processadores de comunicação).

A utilização de multiprocessadores e a redundância em diversos níveis são aplicadas em todos estes sistemas, embora de diferentes maneiras.

Nos sistemas TP 4000, TANDEM 16, PLURIBUS e CCP/USP os recursos redundantes são ativos, o que resulta num aumento da capacida

de computacional da máquina. O sistema ESS-3A mantém o módulo reserva na condição de inativo com a memória sempre atualizada, o que pode ser encarado como um reserva "quente" ("hot standby").

A deteção de falhas e a recuperação de erros são atribuídas a circuitos geradores/verificadores de paridade, temporizadores e rotinas de autodiagnose em todos os sistemas vistos. Estas técnicas são aplicadas aos barramentos de dados que envolvem memórias e dispositivos de E/S.

Apesar das diferenças na arquitetura, todos os sistemas possuem barramento interno duplicado, inclusive a CCP/USP que trabalha com topologia em anel.

Os processadores (UCPs) utilizados apresentam diferentes características: no sistema CCP/USP e TP 4000 é utilizada a UCP de 8 bits em cada processador; no sistema PLURIBUS é utilizada a UCP de 16 bits; e os sistemas ESS-3A e TANDEM 16 possuem processadores microprogramados, o que caracteriza uma velocidade maior na execução de tarefas.

A alocação de processadores dedicados ao controle de "interfaces" de E/S é aplicada no sistema TP 4000, enquanto nos demais sistemas estas "interfaces", embora redundantes, são controladas por processadores que executam tarefas gerais que incluem controle de E/S. Em todos os sistemas as "interfaces" de E/S possuem redundância.

O problema de alimentação é contornado por meio de duas diferentes soluções: uso de fontes independentes para cada módulo que compõe o sistema, como é o caso do sistema PLURIBUS, ou fontes redundantes que alimentam todo o sistema, como é o caso do sistema TP 4000. O sistema TANDEM 16 utiliza duas fontes para o controlador de E/S o que garante uma redundância ao nível do módulo de E/S, além de uma fonte para cada módulo processador.

A manutenção realizada com o sistema ligado ("on-line") também é implementada nos sistemas de forma a evitar paradas na operação para a manutenção de algum módulo defeituoso.

O sistema operacional de cada um destes sistemas tem rotinas especiais de teste e deteção de erros, sendo que o sistema mais dependente dos "programas", apesar das redundâncias de circuito, é o PLURIBUS. Nos demais, os mecanismos voltados para tolerância a falhas estão divididos entre "circuitos" e "programas" com ênfase nos circuitos redundantes e de deteção de falhas.

CAPÍTULO 3

O EQUIPAMENTO MCR

3.1 - INTRODUÇÃO

O Multiprocessador de Comunicação em Rede (MCR) é um equipamento que tem como uma das aplicações integrar os nós da sub-rede de comunicação de dados do Sistema REDACE/INPE.

Sua função é gerenciar a comunicação de dados em um grupo de linhas seriais, implementando para isto os níveis mais baixos do protocolo de comunicação e as rotinas auxiliares de roteamento.

A configuração de um nó completo da sub-rede de comunicação de dados em questão está descrita na Figura 3.1 (Hashioka, 1983).

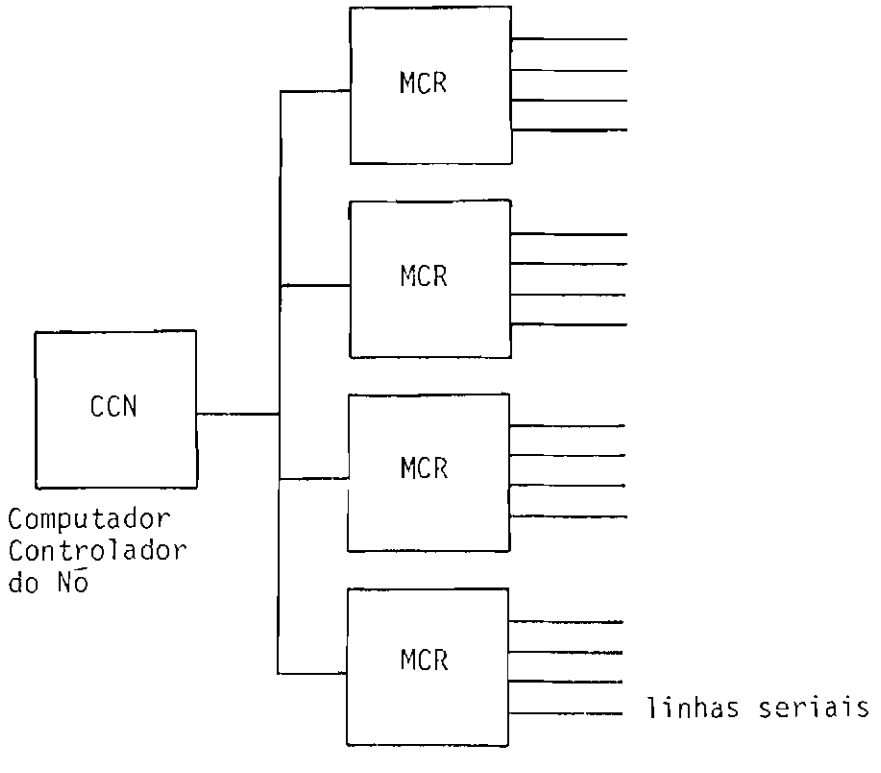


Fig. 3.1 - Configuração de um nó completo do Sistema REDACE.

O MCR é a interface entre os hospedeiros e a sub-rede de comunicação de dados, e pode operar isoladamente de forma a configurar um nó simplificado.

As linhas seriais dos nós servem de acesso a outros nós da mesma sub-rede, ou de outra que opere com protocolo semelhante. Além disto, estas linhas são as vias de acesso aos computadores hospedeiros e às máquinas específicas que estão conectados à sub-rede de comunicação de dados.

O Computador Controlador de Nó (CCN) realiza estatística e controle de fluxo de dados através do nó, exercendo para isto a gerência do barramento interno que interliga os MCRs e o próprio CCN. Através deste barramento, chamado MCR-C-BUS, são efetuadas as trocas de mensagens entre os MCRs e entre cada MCR e o CCN.

O protocolo de comunicação que opera na sub-rede tem seus níveis mais baixos, responsáveis pelo transporte de dados, implementados no nó formado pelo conjunto MCRs e CCN, cabendo aos MCRS a implementação dos níveis que garantem a conexão física e a transferência de dados de forma adequada através das linhas seriais.

As mensagens recebidas através das linhas seriais conectadas aos MCRs são enviadas a seus destinos que podem ser: 1) linha serial pertencente ao mesmo MCR ou 2) linha serial pertencente a outro MCR e CCN. Caso a mensagem recebida não possa ser enviada ao destino devido a problemas temporários de conexão, ela pode ser armazenada temporariamente no CCN, que possui unidades de memória de massa.

3.2 - ARQUITETURA DO MCR

O MCR é formado por um conjunto de unidades de processamento baseadas em microprocessadores que trabalham no esquema mestre-escravo, onde um microprocessador supervisiona o trabalho dos demais.

O diagrama de blocos do MCR é mostrado na Figura 3.2.

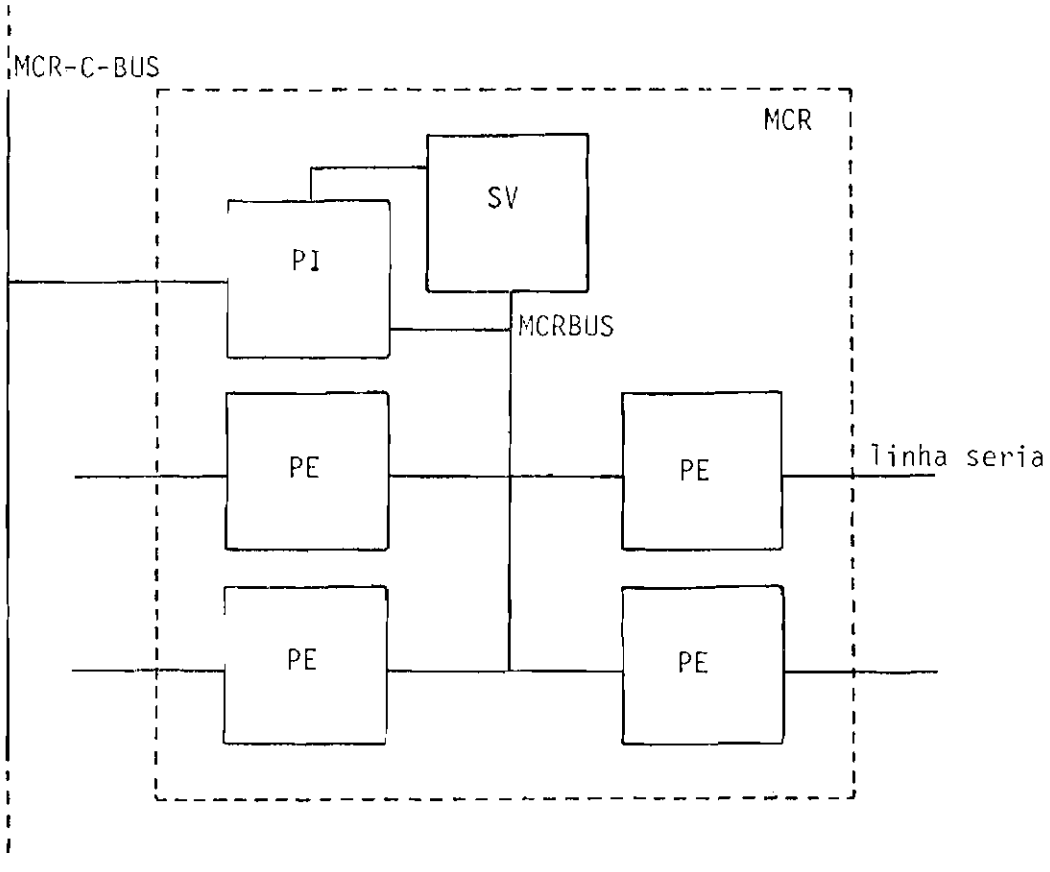


Fig. 3.2 - Diagrama de blocos do MCR.

O módulo denominado SUPERVISOR (SV) e os módulos denominados PORTAS EXTERNAS (PE) possuem, cada um deles, um microprocessador próprio. A PORTA INTERNA (PI), por sua vez, trata de um módulo sem microprocessador próprio e o seu controle está a cargo do SV.

Dentro da hierarquia mestre-escravo, o mestre é o SV enquanto os escravos são as PEs e a PI.

O SV tem como função controlar o fluxo de dados no âmbito interno do MCR, bem como verificar o funcionamento dos demais módulos (PEs e PI), executando rotinas de diagnose.

A tarefa de controlar o fluxo de dados internamente faz com que o SV assuma o total controle do barramento interno do MCR, denominado MCRBUS. É através deste barramento que são executadas as trocas de mensagens entre PE e PE, entre PE e PI, e entre PE e SV.

A PI é a interface entre o MCR e os demais integrantes do nó, ou seja, entre o MCR e o CCN e entre o MCR e os demais MCRs do nó. Esta porta possui três acessos distintos que são:

- CPUBUS que permite a conexão com o SV;

- MCRBUS que permite a conexão com as PEs;

- MCR-C-BUS que permite a conexão com o CCN e demais MCRs.

A PI trata-se de um banco de memórias no qual são armazenadas temporariamente as mensagens que fluem de/para o MCR através do MCR-C-BUS (de/para CCN e demais MCRs do nó). Internamente ao MCR essas mensagens são carregadas/absorvidas da PI através do MCRBUS (PEs) ou CPUBUS (SV).

A PE é responsável pela implementação das interfaces seriais do MCR. Cada PE gerencia uma interface serial, executando para isto as rotinas que fazem parte dos níveis inferiores do protocolo de comunicação que opera na sub-rede.

Através das linhas seriais controladas pelas PEs, são efetuadas as conexões de um nó a outro nó, conexões com computadores hospedeiros da sub-rede, e conexões com máquinas diversas ligadas a estas linhas.

O MCR tem uma arquitetura que suporta até 7 PEs. Os protótipos utilizados durante a fase de desenvolvimento estão configurados com 4 PEs e, para efeito de análise de confiabilidade, neste trabalho, esta será a configuração adotada. As demais configurações, com diferentes número de PEs, são analisadas no Apêndice D.

Desta maneira, num mesmo MCR, têm-se usualmente várias UCPs trabalhando em conjunto. Dado isto, optou-se por utilizar uma CPU padrão que, em conjunto com um "hardware" adicional, configura cada módulo do MCR.

A CPU padrão ocupa fisicamente uma placa em circuito impresso e é conectada à placa que contém o circuito adicional através do barramento CPUBUS. Desta maneira, a PE é formada por duas placas de circuito impresso, uma que contém a CPU padrão e a outra os circuitos adicionais que executam a função específica desta porta.

O conjunto SV+PI também é formado por duas placas de circuito impresso, a CPU padrão e a placa adicional que contém as interfaces, memória e outros circuitos, de maneira a configurar o módulo SV+PI.

Assim, um MCR que opera com 4 PEs, SV e PI é formado por 10 placas de circuito impresso (SV+PI = 2 placas, PE = 2placas).

O objetivo do presente trabalho é analisar unicamente o MCR, considerando sua operação independente dos demais componentes do nó da rede. Desta forma, a Porta Interna (PI) não é considerada na análise da arquitetura atual e na proposta de uma nova arquitetura, pois trata-se de um circuito não-inteligente utilizado apenas para interfacear o MCR com os demais integrantes do nó.

Embora não considerada, a PI é apresentada a seguir, juntamente com os demais módulos (SV e PEs), de forma a ter uma visão global do funcionamento do MCR, internamente e em relação ao nó.

3.2.1 - O SUPERVISOR

O diagrama de blocos do SUPERVISOR é mostrado na Figura 3.3.

O SV possui uma UCP de 8 bits, um banco de memórias com 8K de RAM e 16K de EPROM, onde estão armazenados e são executados os programas que implementam as suas funções.

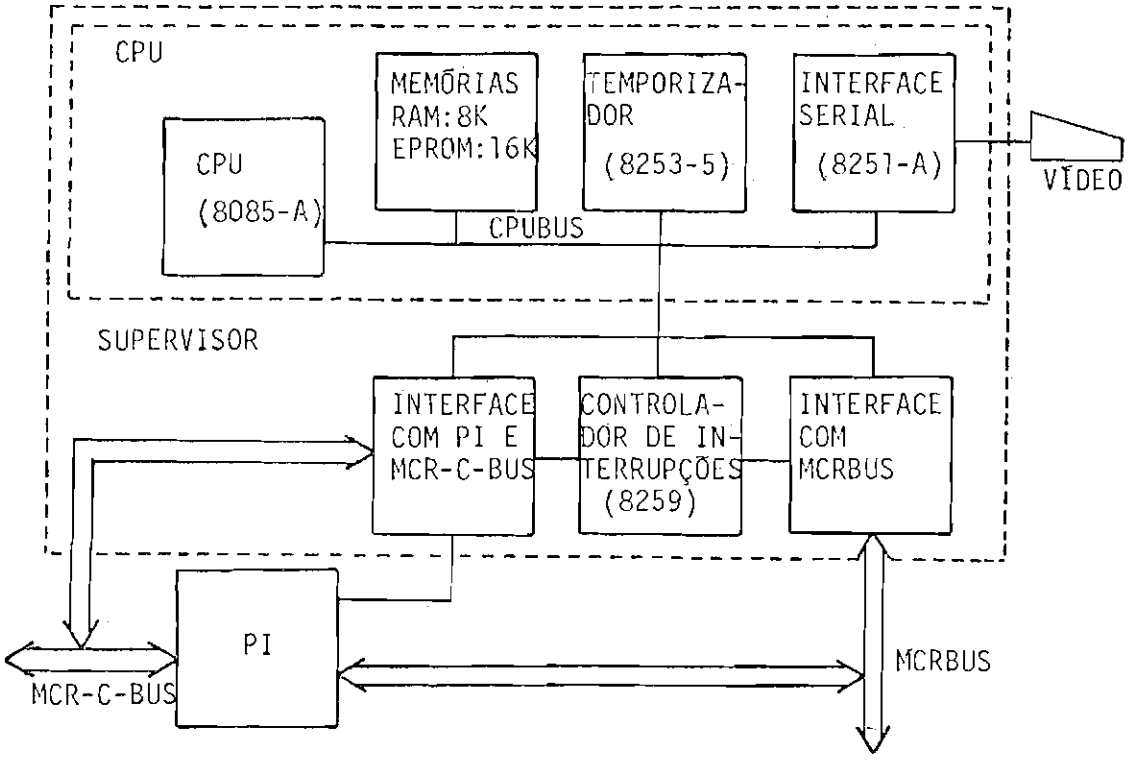


Fig. 3.3 - Diagrama de blocos do Supervisor.

A comunicação com o MCRBUS é feita através de uma interface existente com este barramento. Esta interface possui portas de três estados para os barramentos de dados e endereços, sinais de controle para escrita e leitura através do MCRBUS, e um controlador de interrupções ao qual estão ligadas as interrupções vindas do MCRBUS destinadas ao SV. O temporizador fornece a velocidade para a interface serial, além de gerar interrupção para "timeout" ou mesmo rotinas de diagnose. A interface serial é utilizada para conectar o SV a um terminal de vídeo, utilizado como ferramenta auxiliar na fase de testes. Es

ta interface, durante a operação normal do MCR. serve como opção de acesso do operador ao SV para simples manutenção e testes.

A interface com a PI é formada por portas de três estados controladas pelo SV. Uma vez liberadas estas portas, o SV realiza o acesso à PI através do CPUBUS, que é o barramento interno das UCPs que integram o MCR. Desta maneira, os periféricos que compõem a PI são controlados pelo SV, ocorrendo o mesmo com a memória, que é acessada como uma extensão da memória do próprio SV.

O SV, apesar de controlar o MCRBUS, não tem a função de armazenar ("buffer") as mensagens que trafegam neste barramento. Esta função cabe às PEs e à PI.

3.2.2 - A PORTA INTERNA (PI)

O diagrama de blocos da PI é mostrado na Figura 3.4.

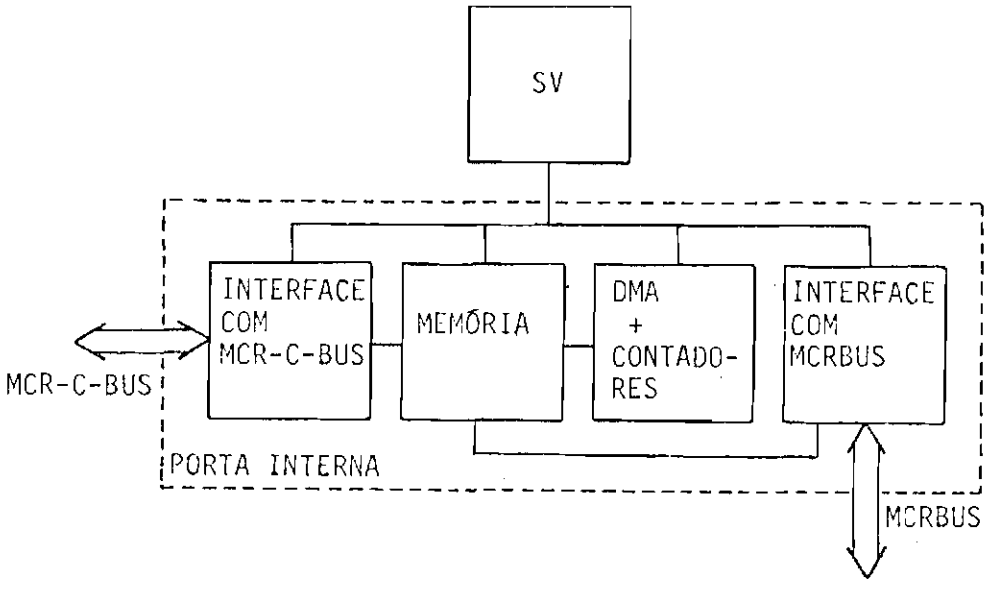


Fig. 3.4 - Diagrama de blocos da Porta Interna.

A PI é formada basicamente por um banco de memórias do tipo acesso aleatório, que constitui a interface entre o MCR e os demais componentes que constituem o nó da sub-rede (CCN+MCRs).

O mecanismo de DMA e contadores serve como suporte na operação de transferência de dados de/para a PI. O controle e a programação destes mecanismos, bem como o acesso à memória compartilhada é feito pelo SV. Apesar deste controle, a PI opera as funções de escrita e leitura de dados em sua memória de forma independente do SV, apenas com o auxílio dos mecanismos de DMA e contadores; estes sim, previamente programados pelo SV.

O acesso à memória da PI pode ser feito por três vias distintas:

- CPUBUS (supervisor);

- MCRBUS (PEs);

- MCR-C-BUS (CCN e MCRs).

A interface com o CPUBUS, ou seja, com o SV, está localizada no próprio SV, enquanto as interfaces para conexão com MCRBUS e MCR-C-BUS estão localizadas na PI.

O SV permite o acesso à PI através de uma e somente uma via por vez. Este controle no acesso está garantido por sinais de "hardware", os quais fazem com que, quando o acesso por uma das vias estiver liberado, os demais estejam bloqueados.

As interfaces com o MCRBUS e o MCR-C-BUS são do tipo três estados. A liberação da interface com o MCRBUS é determinada unica e exclusivamente pelo SV. Já a liberação da interface com o MCR-C-BUS requer dois sinais de controle: um vindo do SV e outro, posterior, vindo do CCN, pois cabe a este o controle das comunicações através do MCR-C-BUS.

Em uma escala hierárquica o CCN possui basicamente a mesma função que o SV. Enquanto o SV controla o fluxo de dados e as comunicações no MCRBUS, o CCN realiza este mesmo controle no MCR-C-BUS. O CCN, porém, possui unidades de armazenamento de massa e outras facilidades não disponíveis no MCR, por este se tratar de um processador de fim específico.

3.2.3 - A PORTA EXTERNA (PE)

A PE implementa a função fim do MCR, que é o controle de linhas seriais para comunicação de dados. O diagrama de blocos da PE é mostrado na Figura 3.5.

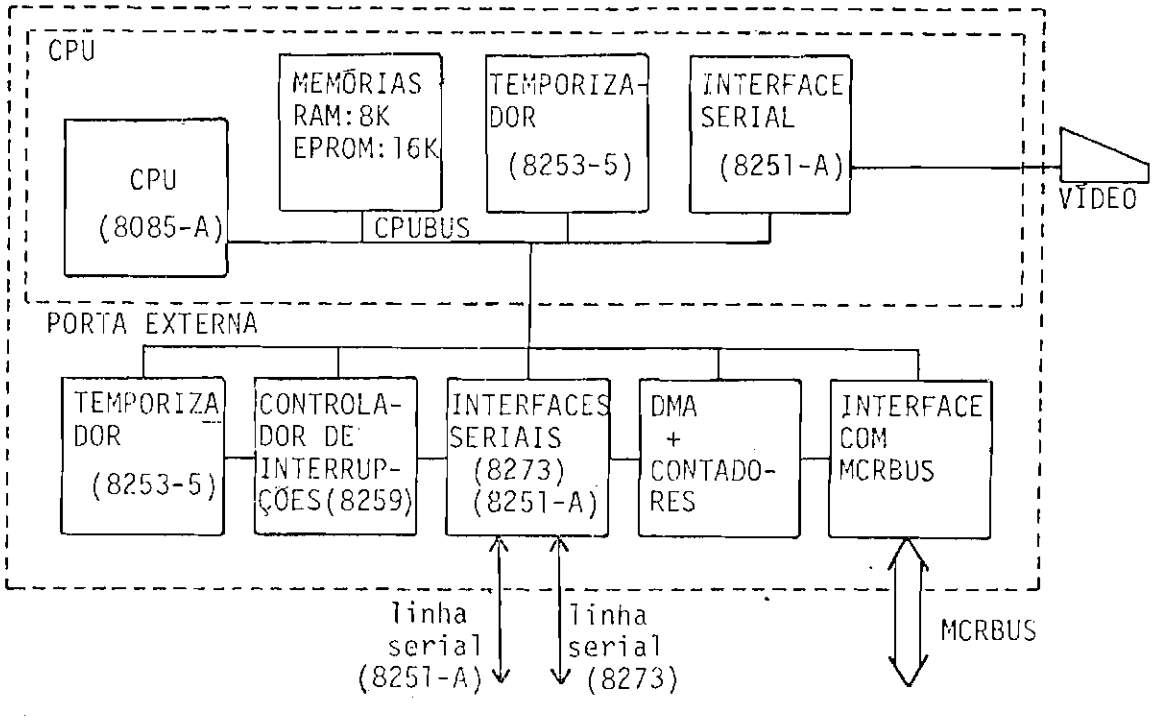


Fig. 3.5 - Diagrama de blocos da Porta Externa.

Este módulo é formado pela placa CPU padrão em conjunto com uma placa adicional denominada placa Unidade Porta Externa. A estrutura da UCP neste caso é igual à utilizada no SV.

O banco de memórias da CPU padrão é destinado ao armazenamento e à execução dos programas que implementam as funções da PE e também ao armazenamento temporário de mensagens recebidas ou a serem enviadas pelas linhas seriais.

Desta maneira, a PE, como um todo, serve como interface serial que implementa níveis inferiores do protocolo de comunicação e como "buffer" temporário das mensagens que transitam por ela.

O temporizador utilizado serve para gerar a velocidade das interfaces seriais utilizadas na PE. Tais interfaces são de dois tipos. A primeira atende às necessidades dos protocolos de comunicação mais sofisticados tais como HDLC, SDLC e X.25. Opera em "full duplex" ou "half duplex" até 64K de "baud rate", gera e verifica automaticamente o CRC ("cyclic redundancy check"), realiza comunicação síncrona e assíncrona, e possui comandos ao nível de quadros (pacotes e cabeçalho). A segunda interface serial é do tipo "USART" e tem como características a operação síncrona e assíncrona, "full" e "half duplex". Porém não tem circuito para geração/verificação de CRC, assim como de comandos ao nível de quadros (Hashioka, 1983).

O mecanismo de DMA e os contadores auxiliam a transferência de dados de/para da PE, tanto no caso de mensagens recebidas/enviadas através do MCRBUS como através da interface serial.

No caso de mensagem a ser enviada através do MCRBUS, o mecanismo de DMA opera no modo avalanche ("burst"), colocando a UCP da PE em estado de alta impedância ("hold") e enviando todo o bloco de dados. Mensagens recebidas através do MCRBUS são carregadas na memória da PE com o auxílio de contadores programáveis. Tais contadores são carregados com o endereço inicial onde a mensagem deve ser escrita e, uma vez iniciada a transferência de dados, a UCP da PE entra em estado

de alta impedância e os contadores são incrementados com pulsos de escrita gerados pela fonte dos dados (outra PE por exemplo). Este sinal é recebido através do MCRBUS e tem dupla finalidade, isto é, carregar os dados na memória e incrementar os contadores.

A transferência de dados através da interface serial utiliza apenas o mecanismo de DMA, tanto na transmissão como na recepção, operando por roubo de ciclo.

3.2.3 - OS BARRAMENTOS DO MCR

O MCR possui três barramentos distintos:

- CPUBUS: barramento padronizado para ligação com a placa CPU padrão;
- MCRBUS: barramento interno do MCR, via pela qual são efetuadas as trocas de mensagens entre PE e PE, entre SV e PE, e entre PI e PE;
- MCR-C-BUS: barramento que interliga MCRs e o CCN.

3.2.3.1 - CPUBUS

O CPUBUS é composto de três grupos distintos de sinais:

- endereços (16 bits);
- dados (8 bits);
- controle.

Os sinais de controle existentes são os sinais padrão para uma UCP: leitura/escrita em memória, interrupção (2 níveis), reconhecimento de interrupção (1 nível), relógio, pedido e reconhecimento de "hold" (alta impedância no barramento da UCP) e sinal de "pronto" ("ready").

Este barramento é a via de ligação entre a placa CPU PADRÃO e o "hardware" adicional localizado em outra placa, os quais juntos irão configurar os módulos que compõem o MCR.

3.2.3.2 - MCRBUS

O MCRBUS é caracterizado por servir de via de comunicação entre módulos que compõem o MCR. Possui dois grupos distintos de sinais destinados a implementar a comunicação entre SV e PEs e a comunicação entre PE e PE, e PE e PI.

O grupo de sinais que implementa a comunicação entre SV e PEs é composto de:

- *Sinais de endereço (6 bits):* Através destes sinais o SV endereça registros de leitura/escrita localizados em cada PE. Estes registros são em número de quatro (8 bits cada) e tem endereços distintos. A PE1, por exemplo, tem os registros 1, 2, 3 e 4, a PE2 os registros 5, 6, 7 e 8, etc. Esta diferenciação nos endereços é obtida através de decodificadores de endereço localizados nas próprias PEs. Tais decodificadores podem ter sua estrutura de decodificação modificada através de "jump's", o que permite a alteração nos endereços dos registros de comunicação com o SV.

- *Sinais de dados (8 bits):* Através destes sinais o SV carrega (escreve) e lê os dados contidos nos registros de comunicação com as PEs.

- *Sinais de controle:*

  - Leitura e escrita: São sinais utilizados para gerar comandos de leitura ou escrita nos registros das PEs.

  - Interrupção: São sete sinais distintos de interrupção que possuem a mesma prioridade de atendimento pelo SV. Estes sinais são ativados sempre que há mensagem disponível nos registros de comunicação entre PE e SV localizados nas PEs. Cada PE tem uma linha de interrupção distinta no MCRBUS.

O grupo de sinais que implementa a comunicação entre PE e PE e entre PE e PI é:

- *Sinais de dados (8 bits):* Através desta via são efetuadas as trocas de dados (mensagens) entre PE e PE, e PE e PI. Este barramento de dados é distinto do barramento de dados utilizado para comunicação entre SV e PEs, e sua utilização é permitida para uma e somente uma troca de mensagens por vez. Não é permitida, por exemplo, a troca de mensagens entre PE1 e PE2, e entre PE3 e PE4 simultaneamente.

- *Sinais de controle e sincronismo:*

  - Pedido/reconhecimento de "hold": O sinal de "hold" é emitido pela porta fonte da mensagem para a porta destino e a transferência de dados inicia-se quando o sinal de reconhecimento ("hlda") é emitido como resposta pela porta destino para a porta fonte de mensagem.

  - Escrita: Sinal emitido pela porta fonte de mensagem para a porta destino. A porta destino utiliza este sinal como sinal de escrita em sua própria memória e também como sinal que incrementa os contadores que geram o endereço durante a transferência de dados.

Além dos sinais utilizados para implementar a comunicação interna ao MCR, o MCRBUS possui sinais de alimentação (VCC = + 5V) e terra (TERRA)

3.2.3.3 - MCR-C-BUS

O MCR-C-BUS é a via de comunicação entre os componentes do nó da sub-rede de comunicação de dados. Tem estrutura idêntica à do MCRBUS, possuindo dois grupos de sinais que implementam a comunicação entre MCR e MCR, e entre CCN e MCRs.

3.3 - CÁLCULO DA CONFIABILIDADE/DISPONIBILIDADE DA ARQUITETURA ATUAL DO MCR

Como já mencionado, este trabalho analisa o equipamento MCR em suas funções básicas de gerenciamento de linhas seriais, tratando-o independentemente dos demais componentes do nó da rede. Para tanto, o cálculo da confiabilidade/disponibilidade da arquitetura atual não leva em consideração a operação da Porta Interna (PI), que é a interface entre o MCR e os demais componentes do nó. Sob este aspecto são considerados para o cálculo o SV e as PEs.

Dado isto, o cálculo da confiabilidade/disponibilidade da arquitetura atual do MCR tem como ponto de partida o cálculo da taxa de falhas de cada módulo e por fim o cálculo da taxa de falhas do próprio MCR.

Para o cálculo da taxa de falhas do MCR foram considerados os valores das taxas de falhas dos componentes que integram as placas que compõem o MCR. As taxas de falhas dos componentes foram calculadas segundo as normas MIL-217-C, com parâmetros dos componentes obtidos nos manuais fornecidos pelos fabricantes. Estes cálculos estão descritos no Apêndice A.

A partir da taxa de falhas de cada componente foi calculada a taxa de falhas de cada placa e, por fim, a taxa de falhas de cada módulo do MCR (SV e PE).

As seguintes considerações foram feitas nos cálculos das taxas de falhas das placas:

- a falha em um componente implica a falha da placa como um todo, considerando-se neste caso a operação degradada como um estado de falha;

- foram desprezadas as taxas de falhas dos resistores e capacitores por serem estas muito menores que as taxas de falhas dos CIs.

A partir destas considerações é obtida a taxa de falhas para cada placa, segundo o modelamento série, onde a taxa de falhas da placa é a soma das taxas de falhas dos componentes que integram esta placa.

Ao nível dos módulos, a taxa de falhas é obtida com a soma das taxas de falhas das placas que compõem este módulo, uma vez que a falha em uma das placas leva o módulo a um estado de falha.

O funcionamento do MCR é considerado dentro das especificações quando todas as linhas seriais a ele conectadas são gerenciadas corretamente. A falha em uma PE, por exemplo, não leva o MCR a uma falha total, pois apenas a(s) linha(s) serial(ais) conectada(s) a esta PE deixa(m) de ser atendida(s). Porém, o não-entendimento a esta(s) linha(s) significa que o equipamento não está operando dentro das especificações estabelecidas, e esta condição é considerada como um estado de falha para os cálculos de confiabilidade.

Sob este aspecto, o cálculo da confiabilidade do MCR é feito utilizando o modelamento série ao nível de módulos (SV e PEs), dado que a falha em um módulo pode levar o equipamento a uma falha total, no caso do SV, ou a uma operação degradada, no caso das PEs, o que é considerado operação fora das especificações e portanto um estado de falha.

A Figura 3.6 ilustra o modelamento utilizado para o equipamento.

Para o cálculo da taxa de falhas do MCR como um todo, foi desprezada a taxa de falhas do barramento interno, por ser esta desprezível diante das taxas obtidas para os módulos que integram o equipamento. Valores típicos para a taxa de falhas em barramentos podem ser encontrados em Blakeslee, 1979.

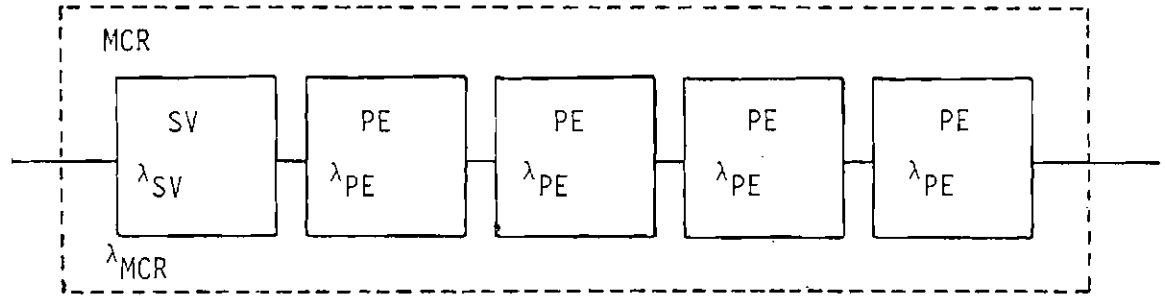


Fig. 3.6 - Modelo utilizado para o cálculo da confiabilidade do MCR.

Os componentes eletrônicos utilizados na montagem do MCR são da classe comercial, e os cálculos das taxas de falhas foram feitos com valores obtidos para esta classe de componentes segundo a norma MIL-217-C

Taxa de falhas por módulos do MCR (valores obtidos no Apêndice A):

SUPERVISOR:

λ_{SV} = 227,7922 f/10^6h.

PORTA EXTERNA:

λ_{PE} = 422, 5132 f/10^6h.

A falha em um dos módulos do MCR provoca um estado de erro para todo o MCR. Desta maneira é aplicado o modelamento "série" para o cálculo da taxa de falhas total do MCR:

$$\lambda_{MCR} = \lambda_{SV} + (4.\lambda_{PE}),$$

λ_{MCR} = 1917,845 f/10^6h.

Para este valor de λ_{MCR} obtém-se:

$$Rmcr(t) = e^{-1917,845t/10^6h}.$$

E a partir de Rmcr(t) obtém-se:

$$MTTF = \frac{1}{\lambda_{MCR}},$$

MTTF = 521,42 horas.

O equipamento MCR tem aplicação prevista na Rede para Controle Espacial (REDACE) da Missão Espacial Completa Brasileira e estará situado fisicamente em estações terrenas e outras instalações do mesmo nível. Os equipamentos destas estações serão supervisionados por operadores e técnicos de manutenção que deverão fazer reparos por ocasião da ocorrência de falhas. O horário previsto para a permanência do técnico de manutenção é o de expediente normal durante os 7 dias da semana, e, sendo assim, o MCR teria cerca de 15 horas diárias sem manutenção imediata. Considerando que a probabilidade de ocorrência de falhas possui uma distribuição constante neste período, o tempo médio de espera para atendimento seria de 7,5 horas. Durante o período normal de trabalho, o tempo de espera para manutenção é nulo. Sendo assim, o tempo médio de espera para manutenção é de $\frac{2}{3} \times 7,5 = \frac{1}{3} \times 0 = 5$ horas. O tempo médio para a manutenção foi estimado de acordo com os valores obtidos com a manutenção dos protótipos em laboratório, e este tempo foi de cerca de 7 horas para todas as placas que compõem o equipamento. O trabalho de manutenção, neste caso, é executado por um técnico especializado que efetua reparos nas placas que apresentam defeitos. Para os cálculos de disponibilidade do MCR, considerou-se este critério de manutenção, com um único técnico efetuando os reparos nas placas, o que caracteriza um servidor único. Outros critérios de manutenção podem ser adotados, porém para os cálculos a seguir considerou-se apenas o critério descrito anteriormente.

A taxa média de reparo do MCR (μ_{MCR}) é dada pelo número de reparos por hora que são feitos neste equipamento. Este valor é dado por $\frac{1}{\text{tempo médio para reparo}}$.

O tempo médio para reparo é obtido somando o tempo médio de espera e o tempo médio para manutenção, e o resultado é 12 horas. Desta maneira a taxa de reparos μ_{MCR} para o MCR é:

$\mu_{MCE} = 1/12$ horas,

$\mu_{MCR} = 83333,3\ r/10^6 h.$

Aplicando este valor de μ_{MCR} e o valor de λ_{MCR} tem-se a disponibilidade "A" do equipamento:

$$A = \frac{\mu_{MCR}}{\mu_{MCR} + \lambda_{MCR}},$$

onde:

A = 97,75%, que corresponde a 197,1 horas/ano de paralização do equipamento.

Uma melhoria imediata nos resultados obtidos pode ser alcançada utilizando componentes mais confiáveis. A utilização de componentes mais confiáveis implica uma maior disponibilidade, porém altera significativamente o custo do equipamento.

Os componentes utilizados são da classe comercial, os quais tem encapsulamento plástico. Componentes mais confiáveis utilizam encapsulamento de cerâmica, sendo que os mais encontrados em nosso mercado são memórias e integrados LSI. Substituindo estes componentes no MCR (permanecendo os TTLs com encapsulamento plástico) têm-se as seguintes taxas de falhas (valores obtidos no Apêndice A):

SUPERVISOR:

λ_{SV_A} = 86,4846 f/10^6h.

PORTA EXTERNA:

λ_{PE_A} = 113,8422 f/10^6h.

Para o MCR:

λ_{MCR_A} = 541,8534 f/10^6h.

O custo total do equipamento, empregando CIs mais confiáveis, está 34% acima do custo obtido com a utilização de componentes usuais do mercado.

Tomando a mesma taxa de reparos utilizada anteriormente, a disponibilidade A_A, obtida com o emprego de componentes mais confiáveis, é:

A_A = 99,35%, que corresponde a 56,94 horas/ano de paralização do equipamento.

Uma análise comparativa indica uma melhoria de 1,63% na disponibilidade às custas de um aumento de 34% no custo.

O emprego de componentes confiáveis é usual quando o equipamento em questão tem aplicação prevista em situações que requerem uma grande disponibilidade. Porém, esta mesma solução esbarra em problemas econômicos, quando o equipamento é produzido em uma escala razoável, já que os componentes mais confiáveis são mais caros.

A utilização de técnicas de tolerância a falhas tende a ser a solução mediadora sob este aspecto. Um equipamento que utiliza componentes normais, porém com redundância ou qualquer outro tipo de auxílio para deteção/correção de falhas, tem sua disponibilidade de uso sensivelmente melhorada e, na maioria das vezes, com um custo menor do que o previsto com a utilização de componentes mais confiáveis.

Uma proposta neste sentido é feita para o equipamento MCR nos capítulos seguintes. A proposta é detalhada, avaliada e por fim comparada, em termos de disponibilidade e custo, com o valores obtidos com a configuração atual do MCR.

CAPÍTULO 4

PROPOSTA DE ARQUITETURA TOLERANTE A FALHAS PARA O EQUIPAMENTO MCR

4.1 - PROBLEMAS DA ARQUITETURA ATUAL

A arquitetura atual do equipamento MCR possui pontos de falha simples que podem levar o sistema todo a uma paralização nas suas operações.

A configuração implementada não prevê nenhum tipo de redundância no "hardware", e os mecanismos de deteção de falhas limitam-se a sinais gerados por temporizadores programáveis e rotinas de diagnose disparadas periodicamente.

Os pontos de falha simples, que podem levar o equipamento diretamente a uma falha total, são o SUPERVISOR (SV) e o barramento interno MCRBUS (o SV controla o MCRBUS que é a única via de comunicação entre os módulos que compõem o MCR). A taxa de falhas do SV foi calculada no Capítulo 2 deste trabalho, enquanto a taxa de falhas do MCRBUS foi considerada desprezível em relação às taxas obtidas para os módulos que compõem o MCR.

As falhas nas PEs causam uma degradação imediata na capacidade de atendimento a linhas seriais no MCR. A manutenção das PEs, em caso de defeito, obriga a uma paralização na operação do MCR para o reparo de placas. Este procedimento leva à conclusão de que a falha em uma PE causa uma degradação imediata no sistema e uma posterior paralização total.

Desta maneira, a falha em qualquer módulo que compõe o MCR na configuração atual leva o sistema direta ou indiretamente a uma paralização total.

As características de operação deste tipo de equipamento requerem em princípio uma alta disponibilidade. A configuração atual conta com uma única alternativa para aumentar a disponibilidade: o uso de componentes mais confiáveis. Esta opção e seus resultados foram motivo de análise na Seção 3.3 deste trabalho. A utilização desta alternativa, no entanto, não contorna o problema de o sistema possuir pontos de falha simples e a provável paralização na operação para manutenção no caso de falhas nas PEs.

Deve-se frisar que, nas análises já realizadas e na proposta de arquitetura a ser feita não é considerada a PI, visto que o trabalho limita-se a analisar unicamente o equipamento MCR, independentemente dos demais equipamentos integrantes do nó. A PI opera como interface entre o MCR e os demais equipamentos do nó.

4.2 - ARQUITETURA PROPOSTA PARA O MCR

A proposta de uma nova arquitetura para o MCR tem como objetivo ser um estudo exploratório, através do qual procura-se contornar os pontos de falha simples apresentados na arquitetura atual, utilizando técnicas de tolerância a falhas como meio de obter uma melhoria nos parâmetros confiabilidade e disponibilidade.

O projeto do equipamento atual envolveu um período de estudo e posterior análise de desempenho para sua validação. A idéia da implementação de mecanismos para aumentar a confiabilidade do MCR parte do princípio de que sua arquitetura básica não deve sofrer modificações profundas com a implementação de mecanismos que visem minimizar os pontos de falha simples.

De uma maneira geral, a implementação de mecanismos de tolerância a falhas em uma arquitetura já existente pode se tornar inviável à medida que requer modificações profundas no projeto até então executado. O MCR atualmente possui todo seu projeto de "hardware" concluído e implementado, e o projeto de "software" definido e sendo implementado. Desta maneira, a viabilidade da proposta de arquite

tura tolerante a falhas está comprometida com o grau de modificações necessárias na arquitetura atual.

A Figura 4.1 mostra a proposta do diagrama de blocos do MCR com uma nova arquitetura que prevê alguns mecanismos para aumento da confiabilidade.

Nesta nova arquitetura o uso de multiprocessadores é mantido de acordo com a arquitetura atual. A técnica aplicada para aumentar a confiabilidade e disponibilidade do equipamento é o uso de módulos redundantes.

A utilização de dois módulos Supervisores, acrescida da deteção de falhas concorrente com a operação, visa contornar o problema de paralização do sistema devido a uma falha simples no SV. A operação destes dois módulos será simultânea, com um SV ativo e outro SV reserva do tipo "reserva quente" ("hot standby"). A inoperância efetiva dos recursos redundantes não compromete o desempenho do sistema, que atende perfeitamente às necessidades operacionais com os atuais recursos, conforme analisado por Hashioka (1983) e Pires (1983) em termos de fluxo e retardo médio.

A redundância proposta é semelhante à utilizada no equipamento ESS-3A (Toy, 1978), analisado na Seção 2.5.3, que prevê uma unidade reserva. Porém no caso do MCR, a unidade reserva opera normalmente executando as mesmas funções da unidade ativa, o que não acontece no equipamento ESS-3A que mantém a unidade reserva inoperante e somente com a memória atualizada de acordo com as atualizações que ocorrem na memória da unidade ativa. O controle do MCRBUS será feito apenas pelo SV ativo, com autorização do "árbitro" implementado. Cabe a este "árbitro" a deteção de falhas nos módulos Supervisores e o eventual chaveamento para o módulo SV reserva em caso de falha do SV ativo. O equipamento ESS-3A trabalha sem o uso da comparação entre as saídas da unidade ativa e da reserva.

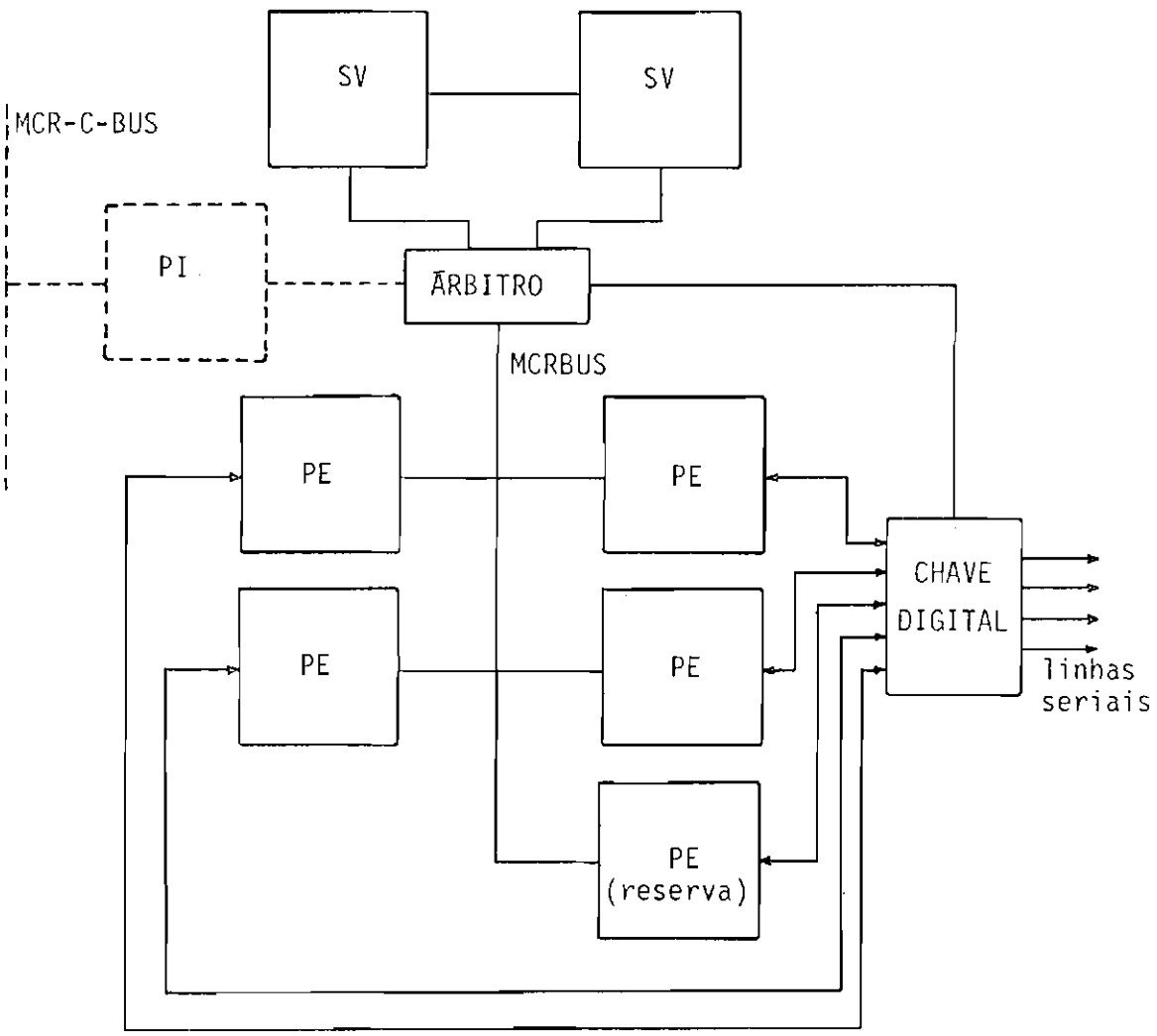


Fig. 4.1 - Diagrama de blocos da arquitetura proposta para o MCR.

O modelo proposto ainda prevê a utilização de uma PE reserva que é chaveada pelo SV para entrar em operação no caso de falha de alguma PE ativa. A carga inicial para configurar uma PE reserva em PE ativa é feita com o auxílio do SV. A aplicação de redundância ao nível de processadores de E/S é utilizada em todos os sistemas analisados na Seção 2.5; no sistema TP 4000 a configuração é semelhante à proposta do MCR, com uma UCP "mestre" (CPU) e processadores dedicados ao tratamento de E/S (LPUs).

Além dos mecanismos propostos na Figura 4.1, a nova arquitetura prevê a opção de manutenção de módulos defeituosos com o sistema ligado ("on-line"), o que implica uma melhora sensível na disponibilidade obtida. Esta característica é encontrada na maioria dos processadores de chaveamento, dada a natureza da operação que exige alta disponibilidade e paradas mínimas para manutenção.

Os novos conceitos a serem implementados têm arquitetura simples, de maneira que sua confiabilidade não comprometa o restante da arquitetura proposta. Estes circuitos são o "árbitro" dos SVs e a "chave digital" ("driver") para chaveamento das PEs.

4.2.1 - O ÁRBITRO

O "árbitro" tem a função básica de decidir qual dos dois SVs em operação deve ter o controle do MCR. Em operação normal o MCR possui um SV ativo e outro reserva. Cabe ao SV ativo controlar o MCRBUS (PEs), a "chave digital" e a PI.

A liberação dos sinais de controle gerados pelos SVs, para que estes atuem efetivamente, é feita pelo "árbitro" através da liberação de portas de alta impedância, as quais estes sinais estão ligados. A Figura 4.2 ilustra este tipo de controle.

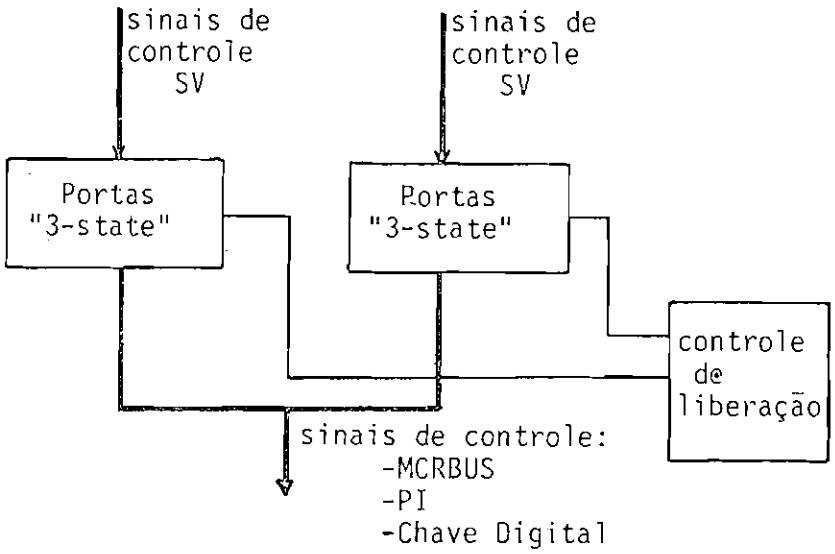


Fig. 4.2 - Controle exercido pelo "árbitro".

O princípio básico de operação do "árbitro" é a comparação dos sinais constantes no barramento de dados dos dois SVs (ativo e reserva) a cada operação de leitura ou escrita na memória e nas portas de E/S. Para que haja sucesso nesta comparação é necessário que os SVs trabalhem sincronizados e isto é conseguido implementando um relógio único ("clock"), o qual está localizado no próprio "árbitro" e é utilizado pelos dois SVs. Este relógio é de 6,144Mhz.

O instante da comparação é determinado através de um circuito que tem como entradas os pulsos: I/OR, I/OM, MEMR e MEMW dos dois SVs e o sinal CLOCK OUT do SV1 que, em condições normais, é o SV ativo. A saída deste circuito é um pulso que indica o instante em que a comparação é válida. O sinal CLOCK OUT é utilizado como referência para que a comparação seja realizada no momento em que o dado é valido no barramento dos SVs. A utilização de apenas um sinal de CLOCK OUT é justificada pelo fato de a comparação feita pelo "árbitro" só ser realizada quando os dois SVs estiverem operando normalmente, pois em caso de falha de um dos SVs o "árbitro" desconecta o SV falho e deixa de realizar a comparação. O procedimento normal de comparação só é reassumido após o reparo do SV que falhou e após a sua volta à operação.

O resultado da comparação é um sinal que possui dois estados:

"0" = comparação correta;

"1" = comparação não-correta.

Em caso de comparação não-correta, o "árbitro" dispara imediatamente uma rotina de autodiagnose nos SVs (Apêndice B), interrompe o procedimento de comparação e entra em um período de espera suficiente para que a rotina seja executada pelos SVs. Após este período de espera o "árbitro" monitora as linhas (uma para cada SV) através das quais os SVs informam o resultado da autodiagnose que pode acusar o bom funcionamento de ambos os SVs, de apenas um SV, ou o mau funcionamento de ambos.

O diagrama de estados do "árbitro" é mostrado na Figura 4.3.

Dado o diagrama de estados tem-se:

ESTADO 0: Indica operação normal dos SVs, com o "árbitro" realizando as comparações a cada operação de escrita e leitura.

Eventos:

- *comparação correta:* O "árbitro" permenece no mesmo estado (ESTADO 0).
- *comparação não-correta:* O "árbitro" dispara a rotina de autodiagnose nos SVs, interrompe o procedimento de comparação e passa para o ESTADO 1.

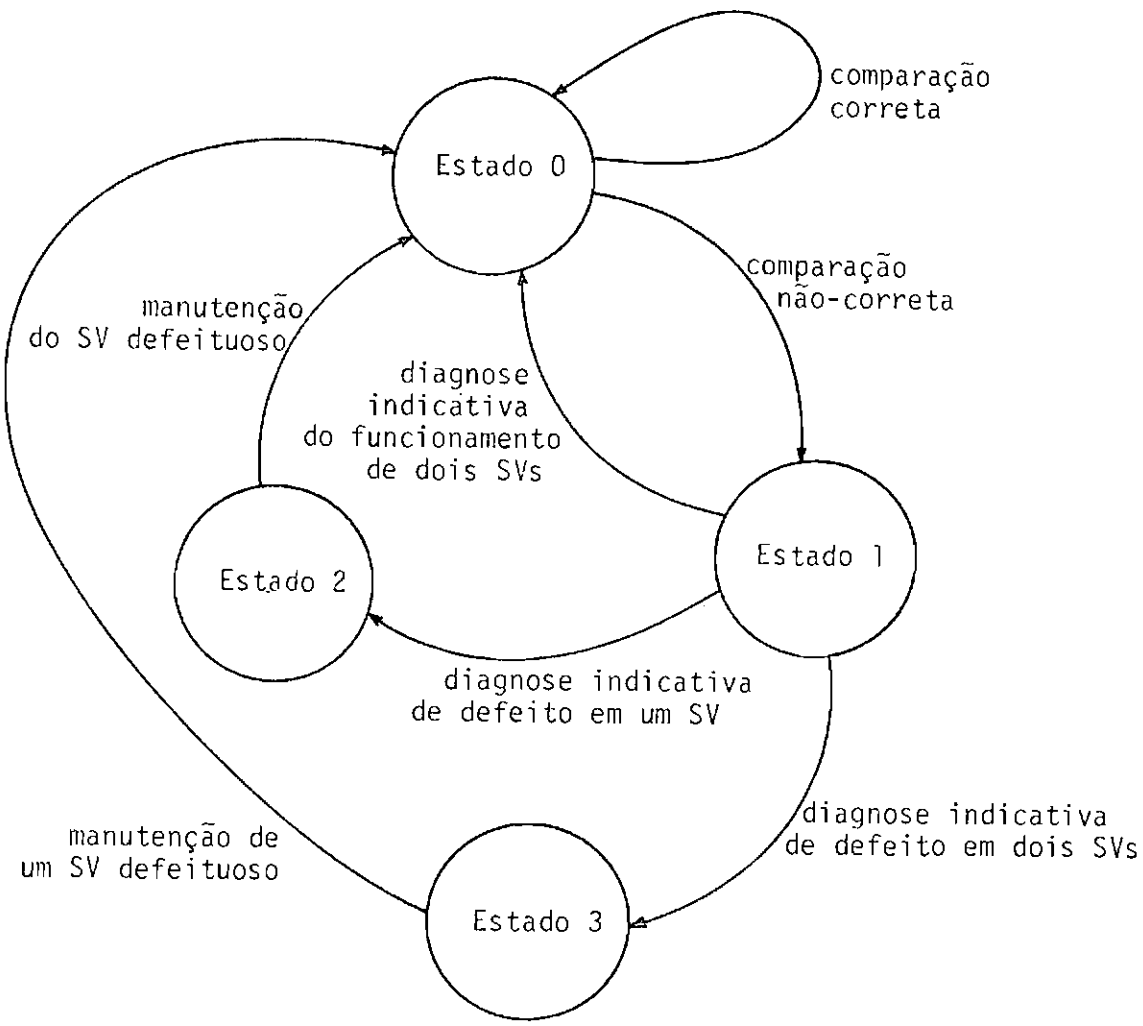


Fig. 4.3 - Diagrama de estados do "árbitro".

ESTADO 1: O "árbitro" entra em um período de espera suficiente para que a autodiagnose seja executada pelos SVs e monitora o resultado desta operação após o período de espera.

Eventos:

- *Resultado da autodiagnose indicativa do funcionamento correto de ambos SVs:* O "árbitro" gera o sinal ARBRESET que inicializa os SVs e o próprio "árbitro", não afetando as PEs. Em seguida volta ao ESTADO 0. Deve ser observado que, neste caso, existe a possibilidade de a rotina de autodiagnose não ter detetado a falha (esta rotina abrange um subconjunto do conjunto de falhas, Apêndice B). Este tipo de problema é abordado nesta Seção 4.2.1 após a descrição dos estados do "árbitro";

- *Resultado da autodiagnose indicativa do funcionamento correto de apenas um SV:* O "árbitro" continua com o procedimento de comparação interrompido, desconecta o SV defeituoso, sinaliza o operador através do painel da máquina e passa para o ESTADO 2;

- *Resultado da autodiagnose indicativa do defeito em ambos SVs:* O "arbitro" continua com o procedimento de comparação interrompido, desconecta os dois SVs, sinaliza o defeito através do painel e passa para o ESTADO 3.

ESTADO 2: O "árbitro" permanece inativo até que seja feita a manutenção do SV defeituoso.

Evento:

- *Manutenção do SV defeituoso:* Uma vez feita a manutenção do SV defeituoso, o "árbitro" precisa ser inicializado, o que provoca uma inicialização geral na máquina. Em seguida o "árbitro" passa para o ESTADO 0.

ESTADO 3: O "árbitro" permanece inativo, mantendo desconectados ambos os SVs.

Evento:

- *Manutenção de um dos dois SVs defeituosos:* Uma vez feita a manutenção em um dos SVs defeituosos, o "árbitro" deve ser inicializado, o que provoca uma inicialização geral na máquina (ESTADO 0). Após inicializado, o "árbitro" volta a realizar a comparação. Porém, esta comparação deve ocorrer apenas uma vez, visto que ainda há um SV defeituoso. Sinalizada a comparação incorreta, o "árbitro" dispara a autodiagnose (ESTADO 1) e deteta a falha em um SV (que ainda não foi reparado) e em seguida interrompe o procedimento de comparação, sinaliza o defeito e passa para o ESTADO 2.

Apenas uma situação não está indicada na descrição dos estados do "árbitro": é o caso em que um SV, embora defeituoso, sinaliza que está operando corretamente no resultado da autodiagnose. Caso isto ocorra, o "árbitro" tende a disparar seguidamente a rotina de autodiagnose, devido ao erro sempre detetado nas comparações.

Este problema é contornado na rotina de autodiagnose (Apêndice B) com o auxílio de um temporizador. Esta rotina possui um registro que é incrementado a cada vez que é executada a autodiagnose, e este registro contador de interrupções é zerado em intervalos de Δt segundos por um comando disparado pelo temporizador existente no SV. Caso o contador de interrupções indique que a autodiagnose foi executada três vezes dentro do intervalo Δt, o SV não a executa novamente e indica estado de erro ao "árbitro".

O circuito do "árbitro" (esquema elétrico), os sinais que compõem a via de conexão entre SVs e "árbitro", e a sua instalação física estão descritos no Apêndice C.

A taxa de falhas para o circuito que compõe o "árbitro" é calculada no Apêndice A a partir do esquema elétrico fornecido no Apêndice C. O valor obtido para esta taxa é:

$$\lambda_{ARB} = 19{,}0533\ f/10^6 h.$$

4.2.2 - A CHAVE DIGITAL

A "chave digital" é o circuito responsável pela conexão/desconexão das linhas seriais externas as PEs.

Na arquitetura proposta o MCR conta com uma PE reserva e quatro PEs ativas. Em caso de falha de uma das PEs ativas, a linha serial conectada a esta PE que falhou é chaveada para a PE reserva. Esta ação é feita pela "chave digital" sob o comando do SV ativo.

A Figura 4.4 ilustra o funcionamento da "chave digital".

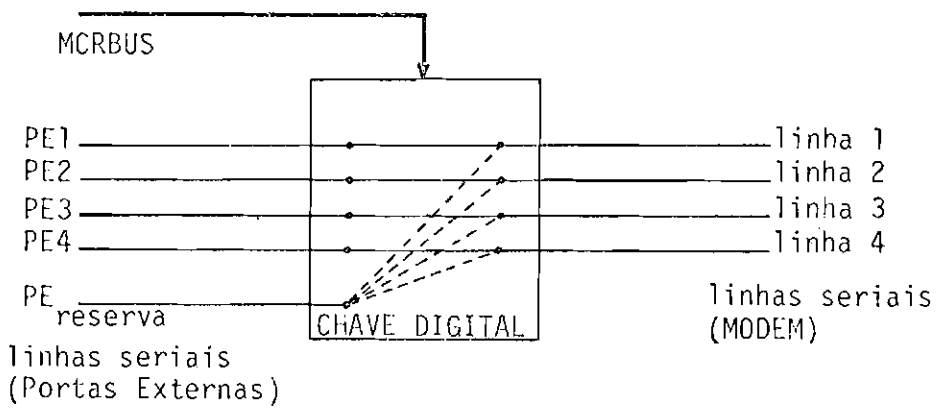


Fig. 4.4 - Funcionamento da "chave digital".

O circuito que configura a "chave digital" (esquema elétrico) e os sinais das vias de conexão PEs - "chave digital" e SVs-"chave digital" estão descritos no Apêndice C.

A taxa de falhas para o circuito da "chave digital" é obtida a partir do esquema elétrico fornecido (Apêndice C) e os cálculos estão descritos no Apêndice A. O valor encontrado é:

$\lambda_{CD} = 16,3077\ f/10^6h.$

O comando de chaveamento de PEs é solicitado pelo SV ativo sempre que é detetada a falha em uma PE. Esta deteção de falhas cabe ao SV que periodicamente dispara uma rotina de autodiagnose existente em cada PE, a qual está descrita no Apêndice B.

4.2.3 - MODIFICAÇÕES NO MCR DEVIDO À NOVA ARQUITETURA

A aplicação da nova arquitetura, com a inclusão do "arbitro", "chave digital", e SV reserva, PE reserva e manutenção "on-line", requer algumas modificações nos circuitos que atualmente compõem o MCR.

O circuito do "árbitro", conforme mencionado na Seção 4.2.1, deverá ocupar a mesma placa que a PI, enquanto o SV passa a ser composta por uma única placa.

O circuito da placa SV deverá ser composto pelo circuito da placa CPU padrão mais os circuitos adicionais do SV que atualmente fazem parte da placa Unidade Porta Interna, que são o controlador de interrupções, decodificadores e interface com o MCRBUS. A utilização de um relógio ("clock") único por parte dos SVs implica a não-utilização de cristal na placa SV e requer a colocação de "drivers" na entrada de relógio da UCP (8085-A). Estes "drivers" já são disponíveis no circuito existente.

A utilização da "chave digital" requer mudanças nas saídas da interface serial das PEs. O nível de tensão nestas saídas não necessita ser convertido para ± 12V (RS 232 C) e os circuitos 1488 e 1489 que fazem esta conversão devem ser substituídos por "drivers" TTL 74LS125, para que a conexão PEs - "chave digital" seja feita em nível TTL (0-5V). A conversão para ± 12V é feita na "chave digital".

A manutenção "on-line" exige a colocação de pequenas chaves nas placas dos SVs e PEs, de maneira a garantir a condição de alta impedância nos "drivers" para os barramentos. Antes de ser instalada no gabinete, a placa precisa ser alimentada (+5V/2A através de cabo puxado da fonte de alimentação) e ter seus "drivers" em alta impedância. Uma vez instalada a placa no gabinete, a chave que garante o estado de alta impedância para os "drivers" deve ser desativada e o circuito inicializado.

As taxas de falhas obtidas para os módulos e as placas que compõem o MCR na nova arquitetura estão calculadas no Apêndice A, e os valores obtidos são:

SUPERVISOR: (A taxa de falhas é dada pela taxa de falhas da placa SV.):

$$\lambda_{SV_P} = 227{,}2922 \text{ f}/10^6\text{h}.$$

PORTA EXTERNA: (A taxa de falhas é dada pela soma das taxas de falhas das placas CPU padrão e Unidades Porta Externa-p.):

$$\lambda_{PE_P} = 421{,}727 \text{ f}/10^6\text{h}.$$

"ÁRBITRO": (A taxa de falhas é dada pela taxa de falhas do circuito do "árbitro", o qual faz parte da placa PI + "arbitro".):

λ_{ARB} = 19,0533 f/10^6h.

"CHAVE DIGITAL": (A taxa de falhas é dada pela taxa de falhas da placa "chave digital".):

λ_{CD} = 16,3077 f/10^6h.

As modificações mencionadas são consideradas e indicadas no Apêndice A, onde são obtidos os valores apresentados.

4.3 - CÁLCULO DA CONFIABILIDADE/DISPONIBILIDADE UTILIZANDO A ARQUITETURA PROPOSTA

Para o cálculo da disponibilidade do MCR, implementando-se a arquitetura proposta, foi utilizado o modelamento por Markov (Billinton, 1983), para o qual levantou-se o diagrama de transição de estados do MCR e as taxas de transição entre estes estados.

Segundo o diagrama levantado para o MCR, mostrado na Figura 4.5 , os estados existentes são:

ESTADO 1: 2 SVs + 5 PEs + N funcionando;

ESTADO 2: 1 SV + 5 PEs + N funcionando, e

1 SV não funcionando;

ESTADO 3: 2 SVs + 4 PEs + N funcionando, e

1 PE não funcionando;

ESTADO 4: 1 SV + 4 PEs + N funcionando, e

1 SV + 1 PE não funcionando;

ESTADO 5: estado de falha.

onde N = "árbitro" + "chave digital".

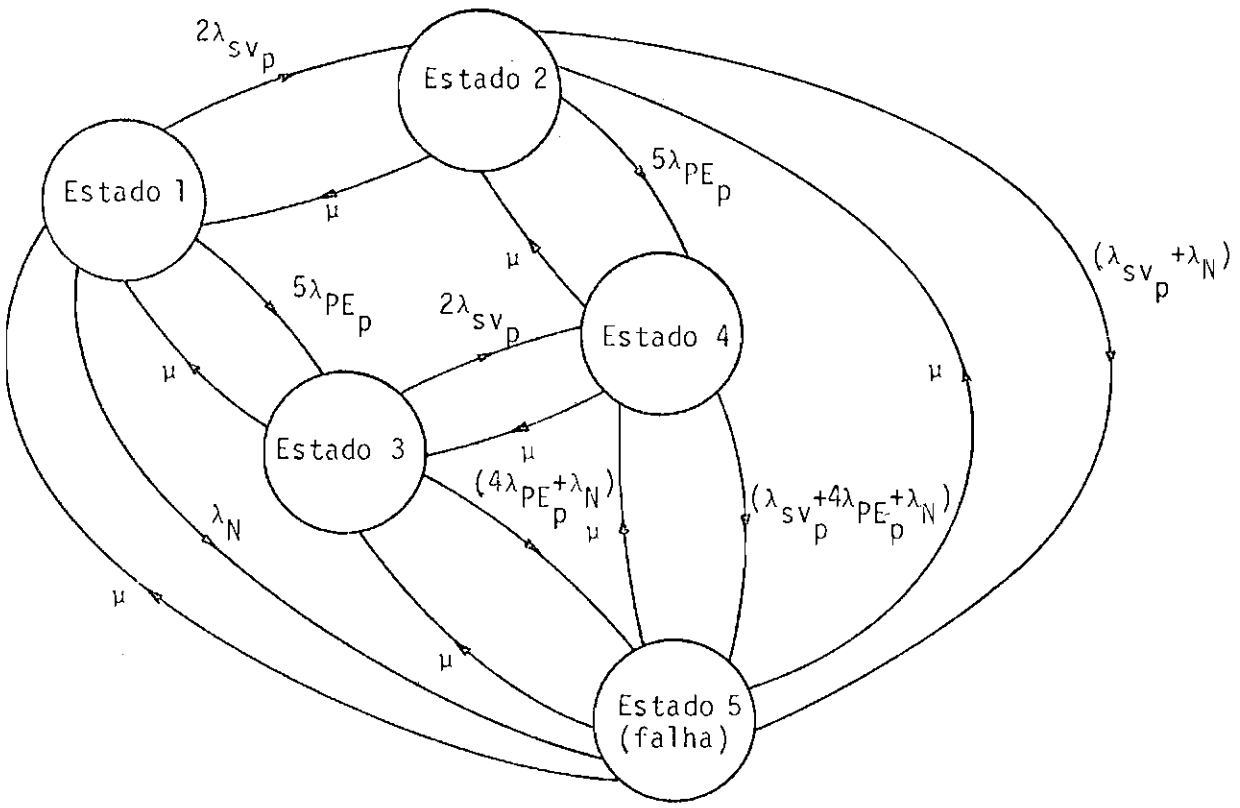


Fig. 4.5 - Diagrama de transição de estado para a arquitetura proposta.

As taxas de transição entre os estados são obtidas a partir das taxas de falhas dos módulos do MCR e a partir da taxa de reparos destes módulos, considerada a mesma para todos e calculada na Seção 3.3 deste trabalho.

As taxas de transição indicadas no diagrama de transição de estados são:

$$\lambda_{SV_P} = 227{,}2922\ f/10^6 h,$$

$$\lambda_{PE_P} = 421{,}727\ f/10^6 h,$$

$$\lambda_N = 35{,}361\ f/10^6 h,$$

$$\mu = 83333{,}3\ r/10^6 h.$$

A partir do diagrama da Figura 4.5 e suas transições, foi levantada a matriz de taxa de transição de estados $\underline{A}$ mostrada a seguir:

$$\underline{A} = \begin{bmatrix} (1-2\lambda_{SV_P} - 5\lambda_{PE_P} - \lambda_N) & 2\lambda_{SV_P} & 5\lambda_{PE_P} & 0 & \lambda_N \\ \mu & (1-\mu-\lambda_{SV_P}-\lambda_N-5\lambda_{PE_P}) & 0 & 5\lambda_{PE_P} & \lambda_{SV_P}+\lambda_N \\ \mu & 0 & (1-\mu-2\lambda_{SV_P}-4\lambda_{PE_P}-\lambda_N) & 2\lambda_{SV_P} & 4\lambda_{PE_P}+\lambda_N \\ 0 & \mu & \mu & (1-2\mu-\lambda_{SV_P}-4\lambda_{PE_P}-\lambda_N) & \lambda_{SV_P}+4\lambda_{PE_P}+\lambda_N \\ \mu & \mu & \mu & \mu & (1-4\mu) \end{bmatrix}$$

Substituindo os valores das taxas na matriz obtida tem-se:

$$A = \begin{bmatrix} -2597,5804 & 454,5844 & 2108,635 & 0 & 35,361 \\ 83333,3 & -87703,0882 & 0 & 2108,635 & 262,6532 \\ 83333,3 & 0 & -85509,1534 & 454,5844 & 1722,269 \\ 0 & 83333,3 & 83333,3 & -168615,1612 & 1949,5612 \\ 83333,3 & 83333,3 & 83333,3 & 83333,3 & 333332,2 \end{bmatrix}$$

Definindo-de o vetor $\underline{P} = [P1\ P2\ P3\ P4\ P5]$, onde P1 = probabilidade limite do sistema estar no estado i (considerando $t \to \infty$), tem-se:

$$\underline{P} \cdot \underline{A} = \underline{P},$$

que significa que as probabilidades Pi para $t \to \infty$ não são afetadas quando multiplicadas pela matriz estocástica $\underline{A}$.

A partir deste princípio tem-se o sistema de equações lineares dado por:

$$\underline{P} \cdot \underline{A} = \underline{P},$$

$$\underline{P} \cdot (\underline{A} - \underline{I}) = 0,$$

Considerando $(\underline{A} - \underline{I}) = \underline{Q}$

tem-se:

$$\underline{P} \cdot \underline{Q} = 0$$

Porém, uma das equações deste sistema é combinação linear das demais e torna-se necessária a utilização de uma condição de contorno. Esta condição é dada por:

$$P1 + P2 + P3 + P4 + P5 = 1,$$

que significa que a soma das probabilidades limites de estar em um dos estados do sistema é 1 (um).

Substituindo a última coluna da matriz $\underline{Q}$, que representa a última equação do sistema, pela equação dada através da condição de contorno, tem-se a matriz modificada $\underline{Qm}$, para a qual:

$$\underline{P} \cdot \underline{Qm} = \underline{B},$$

onde:

$$\underline{Qm} = \begin{bmatrix} -2598,5804 & 454,5844 & 2108,635 & 0 & 1 \\ 83333,3 & -85794,0882 & 0 & 2108,635 & 1 \\ 83333,3 & & -85510,1534 & 454,5844 & 1 \\ 0 & 83333,3 & 83333,3 & -168616,1612 & 1 \\ 83333,3 & .83333,3 & 83333,3 & 83333,3 & 1 \end{bmatrix}$$

e

$$\underline{B} = [0 \quad 0 \quad 0 \quad 0 \quad 1].$$

Após o cálculo matricial, as probabilidades encontradas são:

P1 = 0,969515654,

P2 = 0,005615638,

P3 = 0,024382030,

P4 = 0,000251961,

P5 = 0,000234717.

A disponibilidade A_p do sistema é dada pela probabilidade de este sistema se encontrar em um estado operacional, isto é, não falho.

Neste caso, para o MCR que utiliza a arquitetura proposta tem-se:

$$A = P1 + P2 + P3 + P4,$$

que são as probabilidades de o sistema estar em um estado operacional, ou

$$A_p = 1 - P5.$$

Substituindo os valores obtidos:

$$A_p = 1 - 0,000234717,$$

$$A_p = 0,999765283,$$

ou

$$A_p = 99,977\%,$$

que é o valor da disponibilidade do MCR implementando a arquitetura proposta, a qual corresponde a 2,02 horas/ano de paralização do equipamento.

A confiabilidade $Rmcr_p(t)$ da arquitetura proposta é obtida a partir do modelo série/paralelo levantado para o sistema, o qual é mostrado na Figura 4.6.

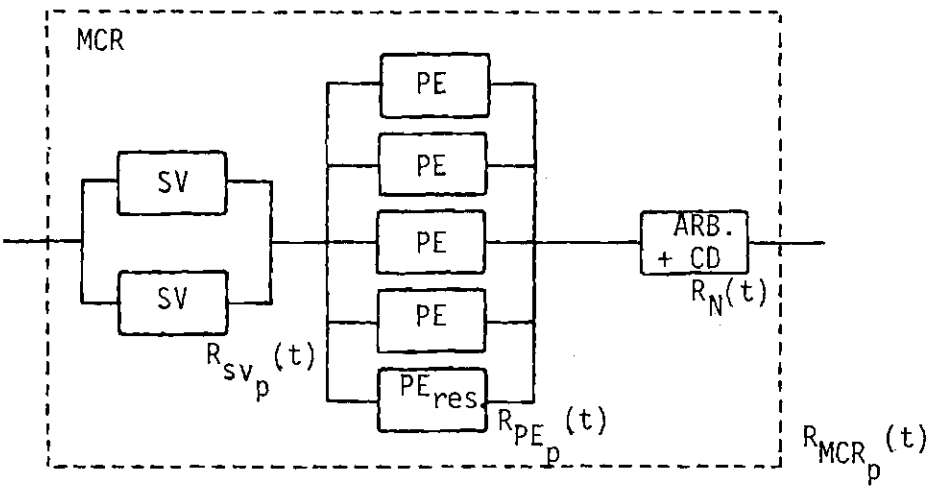


Fig. 4.6 - Modelo para o cálculo da confiabilidade do MCR utilizando a arquitetura proposta.

Segundo o modelo levantado:

$R_{SV_p}(t)$ = confiabilidade do bloco formado pelos SVs (2 SVs em paralelo).

$R_{PE_p}(t)$ = confiabilidade do bloco formado pelas PEs (configuração M de N, ou seja, 4 de 5).

$R_N(t)$ = confiabilidade do Núcleo.

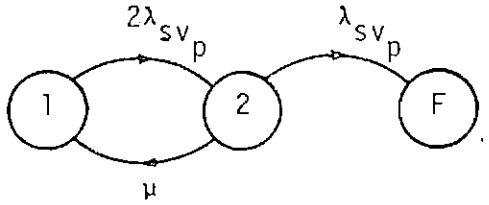
(Núcleo = "árbitro" + "chave digital").

Dados $R_{SV_P}(t)$ e $R_N(t)$, o valor de Rmcr(t) é dado por:

$$Rmcr(t) = R_{SV_P}(t) \cdot R_{PE_P}(t) \cdot R_N(t).$$

Os valores das confiabilidades citadas anteriormente são calculados utilizando o modelo de Markov para o cálculo de confiabilidade (Siewiorek, 1982) para o qual foram levantados os diagramas de transição de estados para os três blocos descritos (SVs, PEs e Núcleo).

O diagrama de transição de estados para o cálculo da confiabilidade do bloco formado pelos SVs é dado por:



onde:

ESTADO 1 = 2 SVs funcionando,

ESTADO 2 = 1 SV funcionando e

1SV não funcionando;

ESTADO F = falha, ou seja, 2 SVs não funcionando.

A partir das equações deduzidas em Siewiorek, 1982, obtêm-se:

$$R_{SV}(t) = \frac{4\lambda_{SV_P}^2}{(3\lambda_{SV_P} + \mu)\,\Delta_{SV} - \Delta_{SV}^2}\, e^{-1/2\,(3\,SV_P + \mu - \Delta_{SV})t} -$$

$$- \frac{4\lambda_{SV_P}^2}{(3\lambda_{SV_P} + \mu)\,\Delta_{SV} + \Delta_{SV}^2}\, e^{-1/2\,(3\lambda_{SV_P} + \mu + \Delta_{SV})t},$$

onde:

$$\Delta_{SV} = \sqrt{\lambda SV_p^2 + 6\lambda_{SV_p}\mu + \mu^2}$$

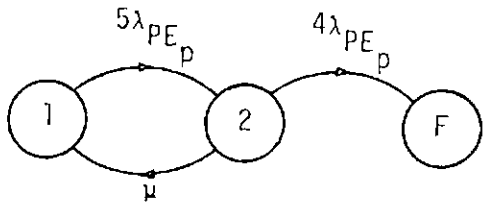
Substituindo os valores $\lambda_{SV_p} = 227{,}2922\ f/10^6h$ e

$\mu = 83333{,}3\ r/10^6h$

e considerando $ta = t/10^6h$ tem-se:

$$R_{SV}(t) = 1{,}0000145\ e^{-1{,}23ta} - 0{,}0000145\ e^{-84013{,}95ta}\ .$$

Para o caso das PEs tem-se o seguinte diagrama de transição de estados:



onde:

ESTADO 1 = 5 PEs funcionando,

ESTADO 2 = 4 PEs funcionando e

1 PE não funcionando;

ESTADO F = falha, ou seja, mais de 1 PE não funcionando.

A partir do diagrama de estados anteriormente apresentado, obtêm-se:

$$R_{PE_P}(t) = \frac{40\lambda_{PE_P}^{\ 2}}{(9\lambda_{PE_P} + \mu)\Delta_{PE} - \Delta_{PE}^{\ 2}} \; e^{-1/2(9\lambda_{PE_P} + \mu - \Delta_{PE})t} -$$

$$- \frac{40\lambda_{PE_P}^{\ 2}}{(9\lambda_{PE_P} + \mu)\Delta_{PE} + \Delta_{PE}^{\ 2}} \; e^{-1/2(9\lambda_{PE_P} + \mu + \Delta_{PE})t} .$$

Substituindo os valores $\lambda_{PE_P} = 421{,}727\ f/10^6h$ e

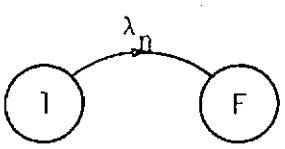
$\mu = 83333{,}3\ r/10^6h$

e $ta = t/10^6h$

tem-se:

$$R_{PE}(t) = 1{,}0004692\ e^{-40{,}843ta} - 0{,}0004692\ e^{-87087{,}998ta} .$$

Por fim, para o bloco Núcleo ("hard core"), o diagrama de transição de estados é:



onde:

ESTADO 1 = "árbitro" + "chave digital" funcionando;

ESTADO F = "árbitro" ou "chave digital", ou ambos não funcionando;

e

$\lambda_N = \lambda_{ARB} + \lambda_{CD}$,

$\lambda_N = 35{,}361\ f/10^6h$.

A confiabilidade neste caso é dada por:

$$R_N(t) = e^{-35,361ta} .$$

Uma vez calculada a confiabilidade de cada bloco, o valor de $Rmcr_p(t)$ é dado por:

$$Rmcr_p(t) = 1,000483371\ e^{-77,436ta} - 0,000469068\ e^{-87124,589ta}$$

$$- 0,0000145068\ e^{-84090,156ta} + 0,0000000068\ e^{-171187,31ta}.$$

Substituindo ta por $t/10^6h$ tem-se:

$$Rmcr_p(t) = 1,000483371\ e^{-77,436t/10^6h} - 0,000469068\ e^{-87124,589t/10^6h}$$

$$- 0,0000145068\ e^{-84090,156t/10^6h} + 0,0000000068\ e^{-171187,31t/10^6h}.$$

A partir de $Rmcr_p(t)$ obtém-se o $MTTF_p$ (tempo médio para falha) para a arquitetura proposta:

$$MTTF_p = \int_0^\infty Rmcr_p(t)\ dt,$$

$$MTTF_p = 0,0129192932 - 10^6 \text{ horas},$$

$MTTF_p$ = 12920,1268 horas, implementando-se a arquitetura para o MCR, o que corresponde a 1,47 ano.

CAPÍTULO 5

ANÁLISE DOS RESULTADOS OBTIDOS E CONCLUSÃO

5.1 - ANÁLISE DOS RESULTADOS OBTIDOS

A análise que se sucede é feita através de um quadro comparativo montado a partir dos resultados obtidos para cada uma das três implementações apresentadas para o MCR.

Estas implementações são:

- arquitetura atual, com uso de componentes comerciais;
- arquitetura atual, com uso de componentes mais confiáveis;
- arquitetura com uso de redundância e componentes comerciais (proposta no Capítulo 4).

Os resultados obtidos são traduzidos nos seguintes parâmetros: disponibilidade, MTTF, e custo. Além destes parâmetros são consideradas na análise e deteção de erros, as implicações devido à implementação prática e a manutenção para as implementações descritas.

a) *Disponibilidade:*

- para a arquitetura atual, com componentes comerciais, obteve-se:

  A = 97,75%,

  o que corresponde a 197,1 horas de paralização por ano;

- para a arquitetura atual, com componentes mais confiáveis, obteve-se:

  A = 99,35%,

  o que corresponde a 56,94 horas de paralização por ano;

- para a arquitetura proposta no Capítulo 4 obteve-se:

  A = 99,977%,

  o que corresponde a 2,02 horas de paralização por ano.

A partir do parâmetro disponibilidade é calculado o tempo estimado de paralização do equipamento. Para o período de um ano há uma redução de 98,96% das horas de paralização, implementando a arquitetura proposta, enquanto a redução é de 71,11% com o uso de componentes mais confiáveis.

b) *MTTF - Tempo Médio para Falha:*

- para a arquitetura atual, com componentes comerciais, obteve-se:

  MTTF = 521,42 horas,

  ou seja, aproximadamente 21,7 dias;

- para a arquitetura atual, com componentes mais confiáveis, obteve-se:

  MTTF = 1845,52 horas,

  ou seja, aproximadamente 2,6 meses;

- para a arquitetura proposta obteve-se:

  MTTF = 12929,13 horas, ou seja, aproximadamente 1,47 ano.

O Tempo Médio para Falhas (MTTF) traduz a confiabilidade do equipamento. Para o caso da arquitetura proposta, o MTTF aumentou em cerca de 24,8 vezes o MTTF obtido para a arquitetura atual. O MTTF obtido com o uso de componentes mais confiáveis é 3,5 vezes o MTTF atual.

c) *Custo:*

- a arquitetura atual com o uso de componentes mais confiáveis tem seu custo 34% superior ao custo da arquitetura atual com componentes comerciais;

- a arquitetura proposta tem um custo 37% superior ao custo da arquitetura atual com componentes comerciais.

Com relação ao custo das implementações, a diferença entre a arquitetura proposta e a arquitetura atual com uso de componentes mais confiáveis não é significativa.

d) *Deteção de erro:*

- a deteção de erros na arquitetura atual é feita através de rotina de autodiagnose, executada periodicamente no Supervisor e nas Portas Externas. A autodiagnose executada no SV cobre parte dos possíveis erros e é disparada através de sinal gerado por um temporizador. Para o caso das PEs, o disparo da autodiagnose é feito pelo SV, também periodicamente.

- Na arquitetura proposta a deteção de erros no SV é concorrente com a operação, dado o mecanismo de comparação implementado através do "árbitro". Uma vez detetado o erro, é disparada a autodiagnose para que seja efetuada a verificação. Nas PEs a deteção de erros permanece com o mecanismo de autodiagnose disparado periodicamente pelo SV.

e) *Implementação prática da arquitetura proposta:*

- a implementação prática de arquitetura proposta não requer mudanças no gabinete que atualmente abriga o MCR.

Em sua forma original, o MCR suporta até 7 PEs operando conjuntamente. Porém, com a implementação da arquitetura proposta, este número fica reduzido a 5 PEs por limitações lógicas, visto que os endereços utilizados por duas PEs são atribuídos à PE reserva e à "chave digital" projetada. Este limite pode ser ampliado efetuando mudanças no circuito de decodificação de endereços para acesso às PEs. Neste caso seriam permitidas 6 PEs ativas e 1 PE reserva (total de 7 PEs). Um número maior de PEs (além de 7) exigiria mudanças no MCRBUS.

f) *Manutenção:*

- o critério de manutenção adotado prevê a presença de um técnico de manutenção durante o expediente normal, o qual efetuará os reparos necessários quando detetada uma falha. Este critério, porém, pode ser revisto com a implementação da arquitetura proposta. Para este caso, a probabilidade de ocorrência de falhas em duas placas do MCR em um curto período de tempo é baixa (conforme visto no Capítulo 4), o que torna dispensável a urgência no reparo a ser executado e dá maior flexibilidade ao esquema de manutenção, permitindo o estabelecimento de manutenção preventiva.

A adoção de outros critérios de manutenção, como por exemplo a substituição de placas durante a ocorrência de falhas, implica uma melhora na taxa de reparos do equipamento e o conseqüente aumento da disponibilidade para todas as implementações. Os cálculos da disponibilidade neste caso não sofrem alteração em sua estrutura, sendo simples o levantamento deste parâmetro para diferentes critérios de manutenção, dado que é modificada apenas a taxa de reparos utilizada nos cálculos.

Uma vez apresentados os resultados obtidos é nítida a vantagem alcançada com a implentação da arquitetura proposta que prevê a utilização de mecanismos de tolerância a falhas. Além da sensível melhoria na disponibilidade e MTTF, esta implementação permite maior flexibilidade com respeito à manutenção. O custo adicional para esta implementação é pouco significativo, dado que o MCR passa a ter características de confiabilidade que o tornam adequado para o uso em rede de comunicação de dados em aplicações espaciais, que exige um alto grau de confiabilidade.

Para as arquiteturas apresentadas, considerou-se o equipamento MCR com quatro PEs ativas e um único critério de manutenção na obtenção da taxa média de reparos. No Apêndice D são apresentados os valores da disponibilidade obtidos para estas arquiteturas, variando

o número de PEs e considerando dois diferentes critérios de manutenção, a partir dos quais se obtêm duas taxas médias de reparos distintas para o equipamento MCR.

5.2 - CONCLUSÃO

O presente trabalho teve como proposta apresentar e analisar uma arquitetura com mecanismos de tolerância a falhas para o equipamento MCR. Os resultados obtidos dão conta da melhora significativa nos parâmetros disponibilidade e confiabilidade deste equipamento.

As técnicas utilizadas para o aumento da confiabilidade incorporadas à arquitetura proposta são de fácil compreensão e, conforme visto no trabalho, a sua implementação é bastante simples, considerando-se os benefícios alcançados.

Esta implementação e os estudos efetuados são considerados para a próxima fase do Projeto REDACE/INPE, a qual, prevê a implantação de mecanismos que aumentam a confiabilidade/disponibilidade da rede de comunicação de dados em aplicações espaciais.

Uma possível extensão deste trabalho é a aplicação de técnicas para o aumento da confiabilidade no nó da rede, considerando um contexto maior, ou seja, o conjunto dos MCRs supervisionados por um Computador Controlador do Nó (CCN). Neste caso a redundância aplicada internamente ao MCR pode ser extendida a todo nó, como por exemplo a duplicação do barramento que interliga os MCRs entre si e ao próprio CCN, redundância na interface entre o MCR e o barramento já citado, e redundância no controlador deste barramento que faz parte do CCN.

Outra possível extensão é o desenvolvimento e aprimoramento das rotinas de autodiagnose do MCR, especificando classes de erros detetáveis e desempenho destas rotinas.

A aplicação de técnicas para o aumento da disponibilidade e confiabilidade é um procedimento necessário a equipamentos desta natureza, utilizados no processamento de comunicação de dados. Embora necessárias, estas técnicas são ainda discriminadas por projetistas em sua grande maioria, que não as usam alegando aumento excessivo no custo, complicações desnecessárias durante o projeto e outras inviabilidades.

Sob este aspecto, o presente trabalho, a despeito de suas imperfeições, procura deixar claras a simplicidade e as vantagens alcançadas com a utilização de técnicas de tolerância a falhas.

REFERÊNCIAS BIBLIOGRÁFICAS

ANDERSON, T.; LEE, P.A. *Fault-tolerance principles and practice.* London, Prentice Hall International, 1981.

ANDERSON, T.; LEE, P.A. Fault-tolerance terminology proposals. In: ANNUAL INTERNATIONAL SYMPOSIUM ON FAULT-TOLERANT COMPUTING, 12, Santa Monica, CA, 22-24 June. *Digest o Papers.* New York, IEEE, 1982, p.29-33.

BARBOSA JR., A.A.; RUGGIERO, W.V.; MOSCATO, L.A.; CAMPOS, E.; STIUBIENER, S. Rede Local no laboratório de sistemas digitais da "EPUSP". In: SIMPÓSIO LATINO AMERICANO SOBRE REDES DE COMPUTADORES, 2., São Paulo, jun. 14-17, 1982. *Anais*, São Paulo, EPUSP, 1982, p.72-80.

BILLINTON, R.; ALLAN, R.N. *Reliability evaluation of engeneering systems:* concepts and techniques. London, Pitman. 1983.

BLAKESLEE, T.R. *Digital design with standart MSI and LSI.* New York, John Wiley. 1979.

BOURICIUS, W.G.; CARTER, W.V.; SCHENEIDER, P.R. *Reliability modeling techniques for self-repairing computer systems.* In: INTERNATIONAL CONFERENCE ON THE ACM, 24., Las Vegas, Aug. 1969. *Proceedings.* New York, ACM, 1969, p.295-309.

COOPER, R.A.; RIVIERE, C. Understanding reliability helps the user optimize network performance. *Data Communications*, 6: 63-67, Jan. 1977.

HASHIOKA, M.H. *Modelo e análise de uma interface de comunicação com processamento distribuído para aplicação em rede de comunicação por comutação de pacotes.* Dissertação de Mestrado em Eletrônica e Telecomunicações, INPE, 1983.

INTEL. *MCS-80/85 Family user's manual.* Santa Clara, CA, USA. 1979.

KAPUR, K.C.; LAMBERSON, L.R. *Reliability in engeneering design.* New York, John Wiley. 1977.

KATSUKI, D.; ELSAM, E.S.; MANN, W.F.; ROBERTS, E.S.; ROBINSON, J.G.; SKOWRONSKI, F.S.; WOLF, E.W. PLURIBUS - An operational fault-tolerant multiprocessor. *Proceedings of the IEEE*, 66 (10): 1146-1159, Oct. 1978.

KATZMAN, J.A. *A fault-tolerant computing system.* TANDEM Computers. 1977.

MAKAM, S.V. *Final report on fault-tolerance aspects of computer communications network processors;* final report. Los Angeles, CA, University of California. Mar. 1979.

US DEPARTMENT OF DEFENSE. Reliability stress and failure rate data for electronic equipment. In: - MIL Standard Handbook. Washington, DC, 1979. (MIL-HDBK-217C).

MUELLER, D. Basic principles for achieving high avaibility. *Data Communications*, 8: 97-99, Oct. 1979.

OPDERBECK, H.; HOFFMEIER, J.H.; SPITZER, R.L. Software architecture for a microprocessor based packet network. *National Computer Conference*, Anaheim, CA, Jun. 1978.

PIRES, L.F. *Simulação de um multiprocessador de comunicação em rede.* Trabalho de graduação em Eletrônica, São José dos Campos, ITA. 1983.

SIEWIOREK, D.P.; SWARZ, R.S. *The theory and practice of reliable system design.* Redford, MA, Digital Press. 1982.

TELENET Communications Processor. *Hardware description.* Washington, DC, Oct. 1977.

TOY, W.N. Fault-tolerant design of local ESS processors. *Proceedings of the IEEE;* 66 (10): 1126-1145. Oct. 1978.

TOY, W.N.; KRAFT, G.D. *Microprogrammed control and reliable design of small computers.* New Jersey; Prentice Hall. 1981.

REFERÊNCIAS COMPLEMENTARES

AVIZIENIS, A. Fault tolerance: the survival attribute of digital systems. *Proceedings of the IEEE*, 66 (10): 1109-1125, Oct. 1978.

DOLL, D.R. How to calculate network reliability. *Data Communications*, 3 (5): 43-49. Jan/Feb. 1975.

HASHIOKA, M.H. Modelo de uma interface de comunicação utilizando multimicroprocessamento . *Simpósio Brasileiro sobre Redes de Computadores*, 2., Campina Grande, PB, 1984.

INTEL. *Peripheral design handbook*. Santa Clara, CA, USA. 1981.

INTEL. *Component data catalog*. Santa Clara, CA, USA. 1982.

MARTINS, E. *Sistemas digitais tolerantes a falhas;* Notas de aula dadas no Instituto de Pesquisas Espaciais (INPE). São José dos Campos, 1º semestre, 1983. 70 p. manuscrito.

NATIONAL SEMICONDUCTOR. *CMOS Data Book*. Santa Clara, CA. 1981.

PAULA JR., A.R.; RODRIGUES, P. Reliable switch architectures. *Networks Communications Processors Seminar*. Los Angeles, CA. Spring 1980.

PAULA JR., A.R. *Evaluation and reliability estimation of distributed architectures for on-board computers*. Dissertation submitted for the degree Doctor of Philosophy in Computer Science. Los Angeles, CA, University of California. 1982.

TEXAS INSTRUMENTS. *The TTL data book for design engineers*. Dallas, Texas. 1981.

WAKERLY, J. *Error detecting codes, self-checking circuits and aplications*. New York, Elsevier North-Holland. 1978.

APÊNDICE A

CÁLCULO DAS TAXAS DE FALHAS PARA O MCR

A.1 - TAXA DE FALHAS PARA OS MÓDULOS DO MCR NA CONFIGURAÇÃO ATUAL

As taxas de falhas para os módulos do MCR foram obtidas a partir da taxa de falhas de cada um dos componentes que pertencem às placas que configuram os módulos. Ao nível de componentes, a taxa de falhas foi calculada segundo as normas MIL-217 C (1979), para as quais foram considerados os seguintes valores para os parâmetros:

fator de aprendizagem $\pi_L = 1$,

fator de ambiente $\pi_E = 2{,}5$,

fator de tensão $\pi_V = 1$.

Estes valores são aplicados a todos os componentes utilizados.

A temperatura de operação dos CIs foi considerada como 35^oC, dentro de gabinete com ventilação forçada.

Os demais parâmetros: fator de qualidade (π_Q), fator de temperatura (π_T), fatores de complexidade (C1, C2 e C3) e fator de técnica de programação em PROM (π_{PT}) foram calculados a partir de dados fornecidos pelos fabricantes através de manuais dos componentes (número de portas, potência dissipada, número de pinos, etc.) e a partir de tabelas da norma MIL-217 C.

Os valores obtidos para os parâmetros e para as taxas de falhas calculadas para os componentes estão indicados nas Tabelas A1, A2 e A3, as quais se referem à placa CPUpadrão, placas Unidade Porta Externa, e Placa Unidade Porta Interna, respectivamente.

A taxa de falhas obtida para cada uma destas placas é o resultado da soma das taxas de falhas dos componentes que as integram, mais as taxas de falhas indicadas para os conectores (borda e cabo) e cristal (se houver). Foram desprezadas as taxas de falhas dos resistores e capacitores por serem estas muito menores que as taxas obtidas para os CIs.

A.1.1 - TAXA DE FALHAS DO SUPERVISOR (SV)

A taxa de falhas do SV é dada pela soma da taxa de falhas da placa CPUpadrão com as taxas de falhas dos componentes que compõem o SV e fazem parte da placa Unidade PI (indicados na Tabela A.3). Estes componentes referem-se ao circuito controlador de interrupções, à interface com MCRBUS e decodificadores, que fazem parte do SV.

Assim:

$$\lambda_{SV} = \lambda_{CPUpadrão} + \lambda_{componentes\ extras},$$

$$\lambda_{SV} = 206{,}4165\ f/10^6h + 21{,}3757\ f/10^6h,$$

$$\lambda_{SV} = 227{,}7922\ f/10^6h.$$

A.1.2 - TAXA DE FALHAS DA PORTA EXTERNA (PE)

A taxa de falhas do módulo PE é dada pela soma das taxas de falhas das placas que compõem este módulo. Estas placas são: CPUpadrão e Unidade Porta Externa, cujas taxas de falhas são indicadas nas Tabelas A1 e A2 respectivamente.

Desta maneira:

$$\lambda_{PE} = \lambda_{CPUpadrão} + \lambda_{Unidade\ Porta\ Externa},$$

$$\lambda_{PE} = 206,\ 4165\ f/10^6h + 216{,}0967\ f/10^6h,$$

$\lambda_{PE} = 422,5132\ f/10^6h.$

A.1.3 - UTILIZAÇÃO DE COMPONENTES MAIS CONFIÁVEIS

Utilizando memórias RAM e componentes LSI com encapsulamento de cerâmica para os módulos do MCR, os valores das taxas de falhas são reduzidos. Os componentes a serem substituídos e suas taxas de falhas são indicados nas Tabelas A.1, A.2 e A.3. Com a utilização de componentes mais confiáveis as taxas de falhas para os módulos são:

Supervisor:

$\lambda_{SV_A} = \lambda_{CPUpadrão_A} + \lambda_{componentes\ extras_A}$,

$\lambda_{SV_A} = 77,4725\ f/10^6h + 9,0121\ f/10^6h,$

$\lambda_{SV_A} = 86,4846\ f/10^6h.$

Porta Externa:

$\lambda_{PE_A} = \lambda_{CPUpadrão_A} + \lambda_{Unidade\ Porta\ Externa_A}$;

$\lambda_{PE_A} = 77,4725\ f/10^6h + 36,3697\ f/10^6h,$

$\lambda_{PE_A} = 113,8422\ f/10^6h.$

e, para o

MCR:

$\lambda_{MCR_A} = \lambda_{SV_A} + (4.\lambda_{PE_A}),$

$\lambda_{MCR_A} = 541,8534\ f/10^6h.$

A.2 - TAXAS DE FALHAS PARA OS MÓDULOS DO MCR IMPLEMENTANDO A ARQUITETURA PROPOSTA

A.2.1 - TAXA DE FALHAS DO SUPERVISOR (SV)

Na arquitetura proposta o módulo SV é constituído por apenas uma placa, denominada placa Supervisor. Esta placa é formada pelo circuito da placa CPUpadrão acrescido dos componentes extras necessários à configuração do SV que estavam contidos na placa Unidade Porta Interna.

Estes componentes são:

CI 74LS04 (1)

CI 74LS08 (1)

CI 74LS32 (3)

CI 74LS138 (1)

CI 74LS245 (4)

CI 8212 (1)

CI 8259 (1)

correspondentes ao controlador de interrupções, decodificadores e interface com o MCRBUS.

Além do acréscimo de componentes, o circuito da CPUpadrão tem sua entrada de relógio ("clock") modificada para receber o relógio ("clock") gerado pelo "árbitro". O cristal deve ser substituído por portas TTL que têm a função de "driver" (INTEL, 1979), conforme indicado na Figura A.1.

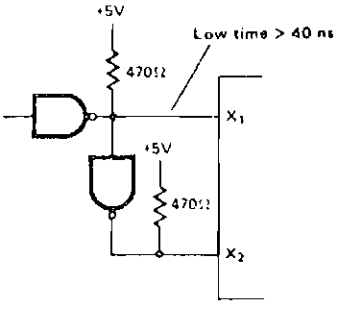


Fig. A.1 - Modificação na entrada de "clock" da UCP 8085-A.

As portas TTL utilizadas já existem disponíveis no circuito da CPUpadrão.

A taxa de falhas da placa SV é dada por:

$$\lambda_{SV_P} = \lambda_{CPUpadrão} - \lambda_{cristal} + \lambda_{componentes\ extras}$$

$$\lambda_{SV_P} = 206{,}4165\ f/10^6h - 0{,}5\ f/10^6h + 21{,}3757\ f/10^6h,$$

$$\lambda_{SV_P} = 227{,}2922\ f/10^6h.$$

A.2.2 - TAXA DE FALHAS DO "ÁRBITRO"

A taxa de falhas do "árbitro" é dada pela taxa de falhas do circuito que compõe o "árbitro". Este circuito está localizado na placa PI + "árbitro" que é constituída pelo circuito que configura a PI e pelo circuito que configura o "árbitro".

Na arquitetura atual o circuito que configura a PI está contido na placa Unidade Porta Interna.

Na aplicação deste trabalho o circuito da PI não é considerado e, neste caso, é considerada apenas a taxa de falhas do circuito do "árbitro" isoladamente, embora os dois circuitos estejam na mesma placa.

A partir dos valores obtidos na Tabela A.4 obtém-se:

$\lambda_{ARB} = 19{,}0533\ f/10^6h.$

A.2.3 - TAXA DE FALHAS DA PORTA EXTERNA (PE)

A taxa de falhas da PE é dada pela soma da taxa de falhas da placa CPUpadrão com a taxa de falhas da placa Unidade PEb que é constituída pelo mesmo circuito que compõe a placa Unidade PE, apenas ocorrendo a substituição dos CIs 1488 e 1489 pelos "drivers" TTL 74LS125 (veja modificações no MCR, Seção 4.2.3).

A taxa de falhas obtida é:

$$\lambda_{PE_p} = \lambda_{CPUpadrão} + \lambda_{Unidade\ Porta\ Externa_p},$$

$$\lambda_{PE_p} = 206{,}4165\ f/10^6h + 215{,}3105\ f/10^6h,$$

$$\lambda_{PE_p} = 421{,}727\ f/10^6h.$$

A.2.4 - TAXA DE FALHAS DA "CHAVE DIGITAL"

A taxa de falhas da "chave digital" é obtida a partir dos valores da Tabela A.5, pela qual:

$\lambda_{CD} = 16{,}3077\ f/10^6h.$

TABELA A.1

TAXA DE FALHAS DA PLACA CPUpadrão

COMPONENTES	QUANT.	Nº DE PORTAS	FATOR DE QUALIDADE π_Q	FATOR DE TEMPERATURA π_T	FATOR DE PROGRAMA π_{PT}	C1	C2	C3	TAXA DE FALHAS f/10^6h
74SL04	2	6	35	0,234		0,0024	0,0004	0,0051	0,5009
74LS08	2	4	35	0,241		0,0019	0,0004	0,0051	0,4973
74SL32	3	4	35	0,247		0,0019	0,0004	0,0051	0,4977
74LS74	2	12	35	0,238		0,0038	0,0005	0,0051	0,5129
74LS138	2	16	35	0,260		0,0046	0,0006	0,0061	0,6281
74LS139	1	18	35	0,260		0,0050	0,0006	0,0061	0,6318
74LS245	3	18	35	2,200		0,0059	0,0006	0,0080	1,1375
74LS257	1	15	35	0,330		0,0044	0,0006	0,0061	0,5371
8212	1	70	35	13,0		0,0100	0,0007	0,0100	5,4863
8212 *			17,5	0,418					0,5413 *
8251-A	1	700	35	18,0		0,0240	0,0011	0,0120	16,2663
8251-A *			17,5	0,453					0,7634 *
8253-5	1	500	35	26,5		0,0210	0,0010	0,0100	20,4400
8253-5*			17,5	0,484					0,6593 *
8085-A *	1	2067	17,5	0,769		0,0370	0,0014	0,0190	1,3085 *
2114 AL4	16	4096bits	35	1,163		0,1370	0,0053	0,0070	6,7403
2114 AL4 *			17,5	0,256					1,1956 *
2732-A *	4	32768bits	17,5	1,675	3,4076	0,1000	0,0042	0,0110	10,6535 *
1488	1	4	35	4,58		0,0310	0,0004	0,0051	0,7658
1489	1	4	35	0,360		0,0019	0,0004	0,0051	0,5039
Conector (placa)	1								0,1000
Conector	1								0,0500
T O T A L									205,4165
									77,4725

OBSERVAÇÕES: 1) (*) = Componentes com encapsulamento de cerâmica.

2) Para todos os componentes consideraram-se: fator de tensão (π_V) = 1, fator de aprendizagem (π_L) = 1,

fator de ambiente (π_E) = 2,5, temperatura de operação dos componentes = 35^oC.

TABELA A.2

TAXA DE FALHAS DA PLACA UNIDADE PORTA EXTERNA

COMPONENTES	QUANT.	Nº DE PORTAS	FATOR DE QUALIDADE π_Q	FATOR DE TEMPERATURA π_T	FATOR DE PROGRAMA π_{PT}	C1	C2	C3	TAXA DE FALHAS f/10^6h
74LS00	2	4	35	0,223		0,0019	0,0004	0,0051	0,4961
74LS04	4	6	35	0,234		0,0024	0,0004	0,0051	0,5009
74LS08	1	4	35	0,241		0,0019	0,0004	0,0051	0,4973
74LS32	3	4	35	0,247		0,0019	0,0004	0,0051	0,4977
74LS74	3	12	35	0,238		0,0038	0,0005	0,0051	0,5129
74LS125	3	4	35	0,330		0,0019	0,0004	0,0051	0,5037
74LS138	9	16	35	0,260		0,0045	0,0006	0,0061	0,6281
74LS139	1	16	35	0,260		0,0050	0,0006	0,0061	0,6318
74LS153	1	16	35	0,258		0,0046	0,0006	0,0061	0,6278
74LS193	4	48	35	0,399		0,0094	0,0009	0,0061	0,7175
74LS245	6	20	35	2,200		0,0050	0,0006	0,0080	1,1375
8212	10	70	35	13,0		0,0100	0,0007	0,0100	5,4863
8212 *			17,5	0,418					0,5413 *
8251-A	1	700	35	18,0		0,0240	0,0011	0,0120	16,2563
8251-A *			17,5	0,453					0,7634 *
8253-5	1	500	35	26,5		0,0210	0,0010	0,0100	20,4400
8253-5 *			17,5	0,484					0,6591 *
8257-5	1	800	35	18,0		0,0250	0,0011	0,0190	17,5008
8257-5 *			17,5	0,453					1,0776 *
8259-A	1	700	35	10,5		0,0190	0,0010	0,0120	8,120
8259-A *			17,5	0,399					0,7014 *
8273	1	1000	35	72,0		0,0280	0,0012	0,0190	72,3275
8273 *			17,5	0,613					1,1841 *
1488	1	4	35	4,58		0,0019	0,0004	0,0051	0,7858
1489	2	4	35	0,340		0,0019	0,0004	0,0051	0,5039
Conector (placa)	1								0,1000
Conector	1								0,0500
T O T A L									216,0967 36,3697 *

OBSERVAÇÕES: 1) (*) = Componentes com encapsulamento de cerâmica.
2) Para todos os componentes consideraram-se: fator de tensão (π_V) = 1, fator de aprendizagem (π_L) = 1,
fator de ambiente (π_E) = 2,5, temperatura de operação dos componentes = 35^oC.

TABELA A.3

TAXA DE FALHAS DA PLACA UNIDADE PORTA INTERNA QUE DISCRIMINA OS COMPONENTES DO SUPERVISOR

COMPONENTES	QUANT.	Nº DE PORTAS	FATOR DE QUALIDADE π_Q	FATOR DE TEMPERATURA π_T	FATOR DE PROGRAMA π_{PT}	C1	C2	C3	TAXA DE FALHAS $f/10^6h$
74LS00	2	4	35	0,223		0,0019	0,0004	0,0051	0,4961
74LS04	3+1(SV)	6	35	0,234		0,0024	0,0004	0,0051	0,5009
74LS08	2+1(SV)	4	35	0,241		0,0019	0,0004	0,0051	0,4973
74LS11	1	3	35	0,232		0,0015	0,0004	0,0051	0,4934
74LS27	1	3	35	0,232		0,0015	0,0004	0,0051	0,4934
74LS32	5+3(SV)	4	35	0,247		0,0019	0,0004	0,0051	0,4977
74LS74	2	12	35	0,238		0,0038	0,0005	0,0051	0,5129.
74LS125	4	4	35	0,338		0,0019	0,0004	0,0051	0,5037
74LS138	10+1(SV)	16	35	0,260		0,0046	0,0006	0,0061	0,6281
74LS139	1	18	35	0,260		0,0050	0,0006	0,0061	0,6318
74LS193	4	48	35	0,399		0,0094	0,0009	0,0061	0,7175
74LS245	9+4(SV)	18	35	2,200		0,0050	0,0006	0,0080	1,1375
2114 AL4	16	4096 bits	35	1,163		0,1370	0,0063	0,0070	6,7403
2114 AL4 *			17,5	0,256					1,1956 *
8212	11+1(SV)	70	35	13,0		0,0100	0,0007	0,0100	5,4863
8212 *			17,5	0,418					0,5413 *
8257-5	1	800	35	18,0		0,0250	0,0011	0,0190	17,5088
8257-5 *			17,5	0,453					1,0766 *
8259-A	1(SV)	700	35	10,5		0,0190	0,0010	0,0120	8,120
8259-A *			17,5	0,399					0,7014 *
Conector (placa)	1(PI e SV)								0,1000
Conector	1								0,0500
T O T A L									215,8626 56,3212 * PI
									21,3757 9,0121 * SV

OBSERVAÇÕES: 1) (*) Componentes com encapsulamento de cerâmica.
2) Para todos os componentes consideraram-se: fator de tensão (π_V) = 1, fator de aprendizagem (π_L) = 1,
fator de ambiente (π_E) = 2,5, temperatura de operação dos componentes = 35°C.

TABELA A.4

TAXA DE FALHAS DO CIRCUITO DO ÁRBITRO

COMPONENTES	QUANT.	Nº DE PORTAS	FATOR DE QUALIDADE π_Q	FATOR DE TEMPERATURA π_T	FATOR DE PROGRAMA π_{PT}	C1	C2	C3	TAXA DE FALHAS $f/10^6h$
74LS04	1	6	35	0,234		0,0024	0,0004	0,0051	0,5009
74LS08	3	4	35	0,241		0,0019	0,0004	0,0051	0,4973
74LS09	1	4	35	0,241		0,0019	0,0004	0,0051	0,4973
74LS32	2	4	35	0,247		0,0019	0,0004	0,0051	0,4977
74LS74	3	12	35	0,238		0,0038	0,0005	0,0051	0,5129
74LS85	2	31	35	0,310		0,0071	0,0008	0,0061	0,6802
74LS125	1	4	35	0,338		0,0019	0,0004	0,0051	0,5037
74LS245	8	18	35	2,200		0,0050	0,0006	0,0080	1,1375
CD4069	1	6	35	0,469		0,0041	0,0004	0,0051	0,5486
CD4040	2	132	35	0,713		0,0123	0,008	0,0061	0,9082
Cristal	1								0,5000
Conector (placa)	1								0,1000
Conector	1								0,0500
T O T A L									19,0539

OBSERVAÇÃO: Para todos os componentes consideraram-se: fator de tensão (π_V) = 1, fator de aprendizaem (π_L) = 1, fator de ambiente (π_E) = 2,5, temperatura de operação dos componentes = 35°C.

TABELA A.5

TAXA DE FALHAS DO CIRCUITO DA CHAVE DIGITAL

COMPONENTES	QUANT.	Nº DE PORTAS	FATOR DE QUALIDADE π_Q	FATOR DE TEMPERATURA π_T	FATOR DE PROGRAMA π_{PT}	C1	C2	C3	TAXA DE FALHAS $f/10^6h$
74LS02	1	4	35	0,226		0,0019	0,0004	0,0051	0,4963
74LS08	1	4	35	0,241		0,0019	0,0004	0,0051	0,4973
74LS75	1	24	35	0,260		0,0060	0,0007	0,0061	0,6469
74LS138	1	16	35	0,260		0,0046	0,0006	0,0061	0,6281
74LS244	8	10	35	0,590		0,0034	0,0005	0,0080	0,8140
1488	4	4	35	4,58		0,0019	0,0004	0,0051	0,7858
1489	8	4	35	0,340		0,0019	0,0004	0,0051	0,5039
Conector (placa)	1								0,1000
Conector	5								0,0500
T O T A L									16,3077

OBSERVAÇÃO: Para todos os componentes consideraram-se: fator de tensão (π_V) = 1, fator de aprendizagem (π_L) = 1, fator de ambiente (π_E) = 2,5, temperatura de operação dos componentes = 35°C.

APÊNDICE B

ROTINAS QUE IMPLEMENTAM Á AUTODIAGNOSE NO SUPERVISOR E PORTA EXTERNA

As rotinas de autodiagnose a serem implantadas no SV e PEs têm por objetivos verificar a ocorrência ou não de erros nas partes testáveis do circuito que compõe cada um destes módulos e servir como base para o cálculo de tempo de execução da autodiagnose, parâmetro utilizado pelo "árbitro".

Dado que existem partes não-testáveis no circuito, a autodiagnose deteta um subconjunto do conjunto total de erros possíveis de ocorrer. A porcentagem de erros detetada pela rotina de autodiagnose pode ser estimada por simulação. Contudo, este estudo extrapola o objetivo deste trabalho.

B.1 - ROTINA DE AUTODIAGNOSE DO SUPERVISOR

A rotina de autodiagnose do SV abrange a EPROM, RAM, periféricos e UCP.

a) Teste da EPROM:

A EPROM do SV possui "check sums code" e sendo assim seu teste consiste na verificação dos "check sums" de cada bloco de memória. Os blocos são de 1K"bytes" e no final da cada bloco existe um "check sums code" a ser verificado. O número total de blocos é 16.

b) Teste da RAM:

A memória RAM é de 8K"bytes" e os testes executados são:

- teste de bit preso em "0" (realizado "byte" a "byte");

- teste de bit preso em "1" (realizado "byte a byte");

- teste de bit preso com bit adjacente (realizado "byte" a "byte");

- teste nas vias de seleção do integrado ("chip select" e endereços).

Esta memória é dividida em blocos de 1K "bytes", cada bloco com uma via de seleção de integrado (sinal de "chip select") distinto. O número total de blocos é 8.

c) - Teste dos periféricos:

O SV possui como periféricos o temporizador 8253, o controlador de interrupções 8259 e a interface serial 8251. O teste destes periféricos é feito através de leitura de "status" (8259 e 8251) e excitação para executar uma função (8253). Juntamente com o teste do CI 8259 é feito um teste do circuito extra que permite mascaramento de interrupções no MCRBUS.

d) Teste da UCP:

O teste da UCP realiza operações lógicas aritméticas e de transferência de dados utilizando os registros de uso geral e o acumulador.

A rotina de autodiagnose do SV, a cada vez que é executada incrementa um contador denominado "contador de falhas". Este contador é testado antes da execução das sub-rotinas que testam o SV e, caso o valor indicado neste contador, seja menor que 3 (três), as sub-rotinas que testam o SV não são executadas e a indicação de erro é feita ao "árbitro".

O "contador de falhas" é zerado periodicamente e o intervalo de tempo para esta ação é dado por um dos contadores do 8253.

O tempo estimado para a execução de autodiagnose do SV é de 467 mseg, considerando-se um total de 1435000 estados e cada estado durando 325,5 nseg (valores obtidos para um "clock" de 6,144 MHz para a UCP 8085-A). Desta maneira, o procedimento para zerar o "contador de falhas" deve ser executado em períodos Δt > três vezes o tempo de execução da autodiagnose, ou seja:

$\Delta t > 3 \times 467$ mseg,

$\Delta t > 1{,}4$ seg, que é o intervalo de tempo a ser dado por um dos contadores do temporizador 8253.

O fluxograma da rotina de autodiagnose do SV é mostrado na Figura B.1 e os fluxogramas das sub-rotinas da rotina de autodiagnose são mostrados nas Figuras B.2 (teste UCP), B.3 (teste EPROM), B.4 (teste RAM/ parte 1), B.5 (teste RAM/ parte 2), B.6 (teste RAM/parte 3), e B.7 (teste periféricos).

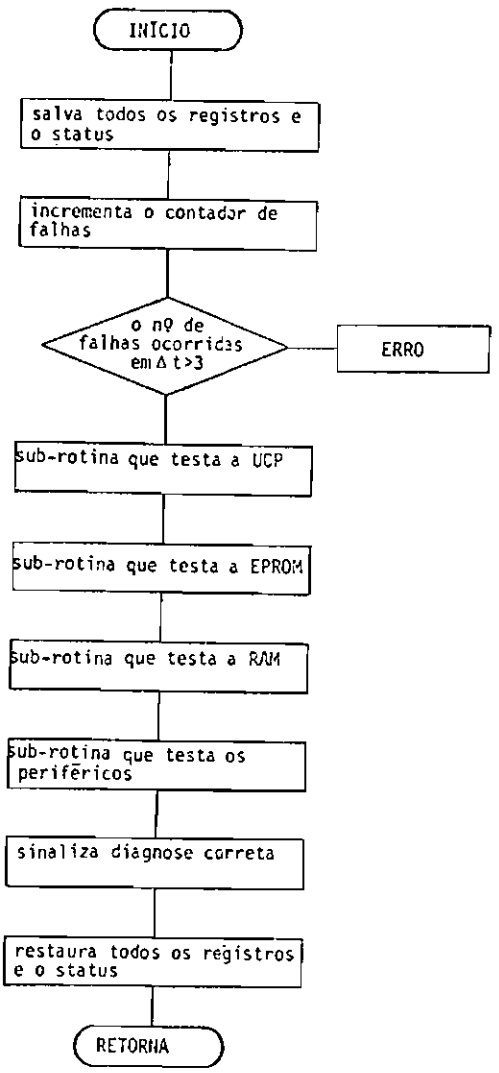


Fig. B.1 - Fluxograma da rotina de autodiagnose do Supervisor.

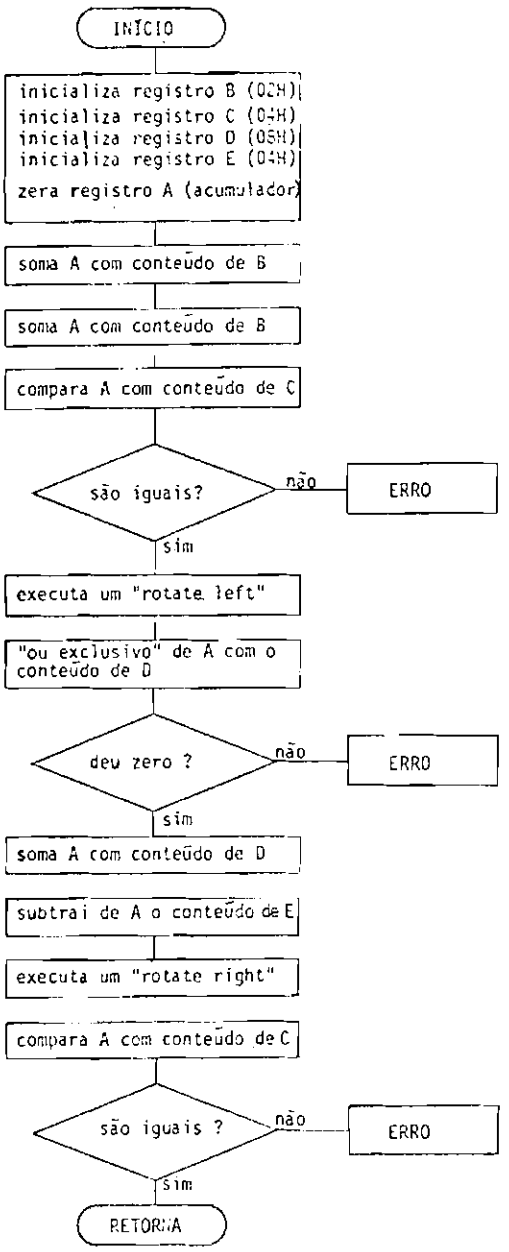


Fig. B.2 - Fluxograma da sub-rotina de teste da UCP.

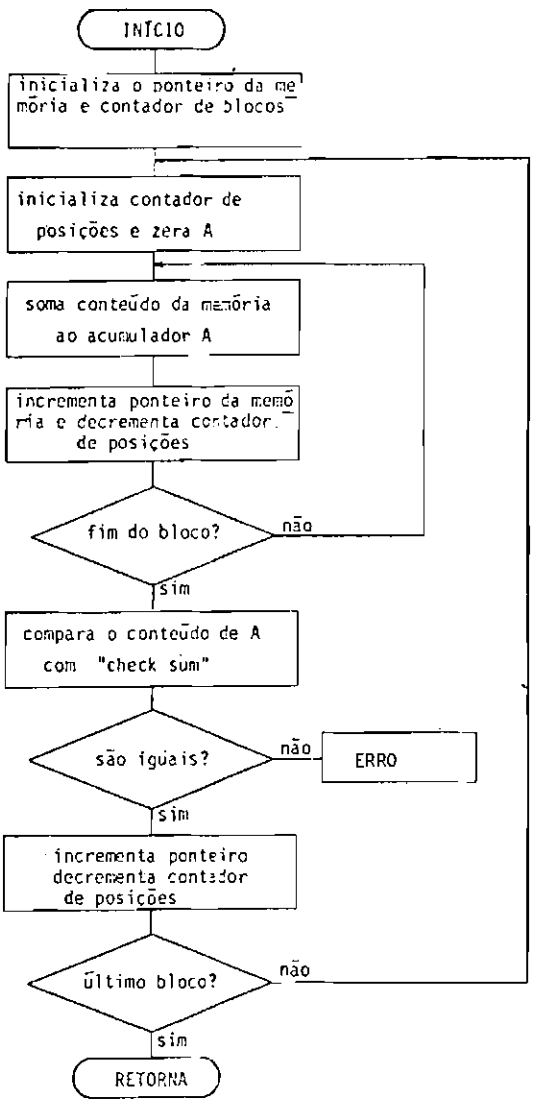


Fig. B.3 - Fluxograma da sub-rotina de teste da EPROM.

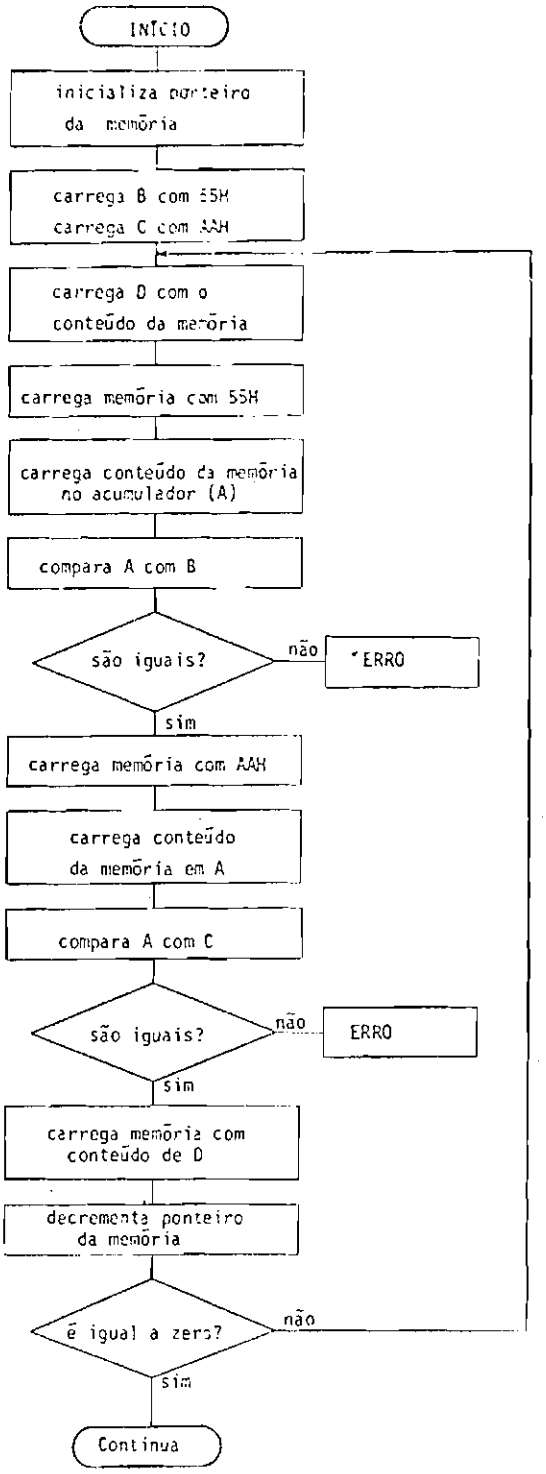


Fig. B.4 - Fluxograma da sub-rotina de teste da RAM.
Parte 1 : teste de bit preso em zero,
teste de bit preso em um,
teste de adjacência.

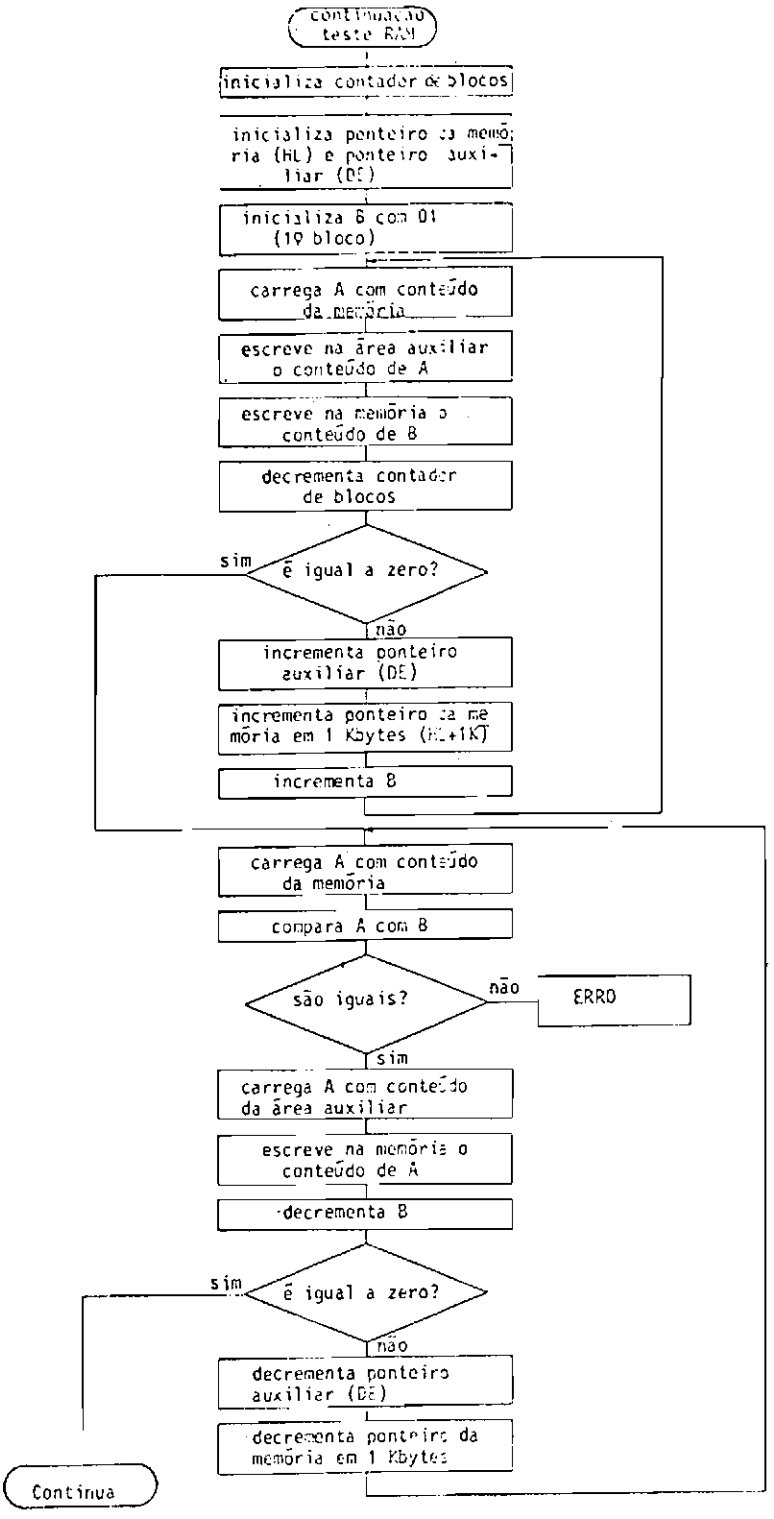


Fig. B.5 - Fluxograma da sub-rotina de teste da RAM.
Parte 2 : teste de via de seleção (chip select).

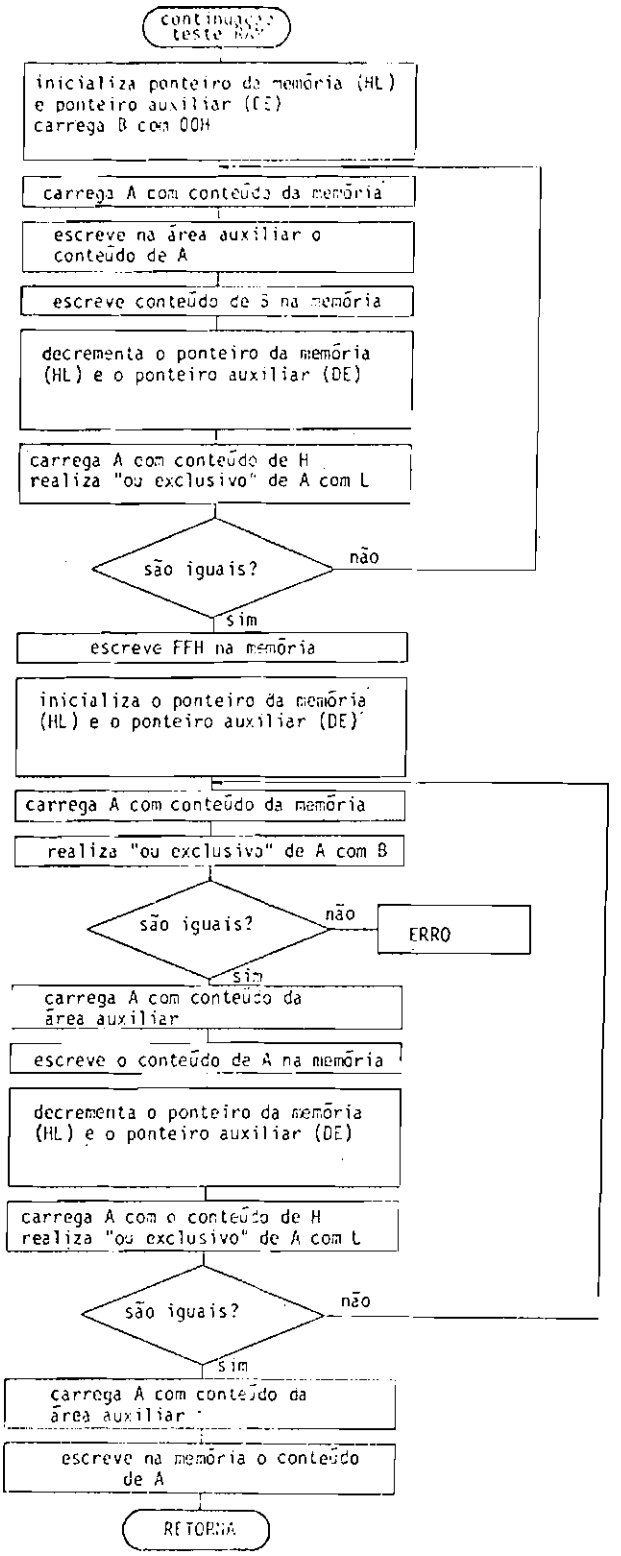


Fig. B.6 - Fluxograma da sub-rotina de teste da RAM.
Parte 3: teste de linha de endereço presa ou com erro de adjacência (A0-A9).

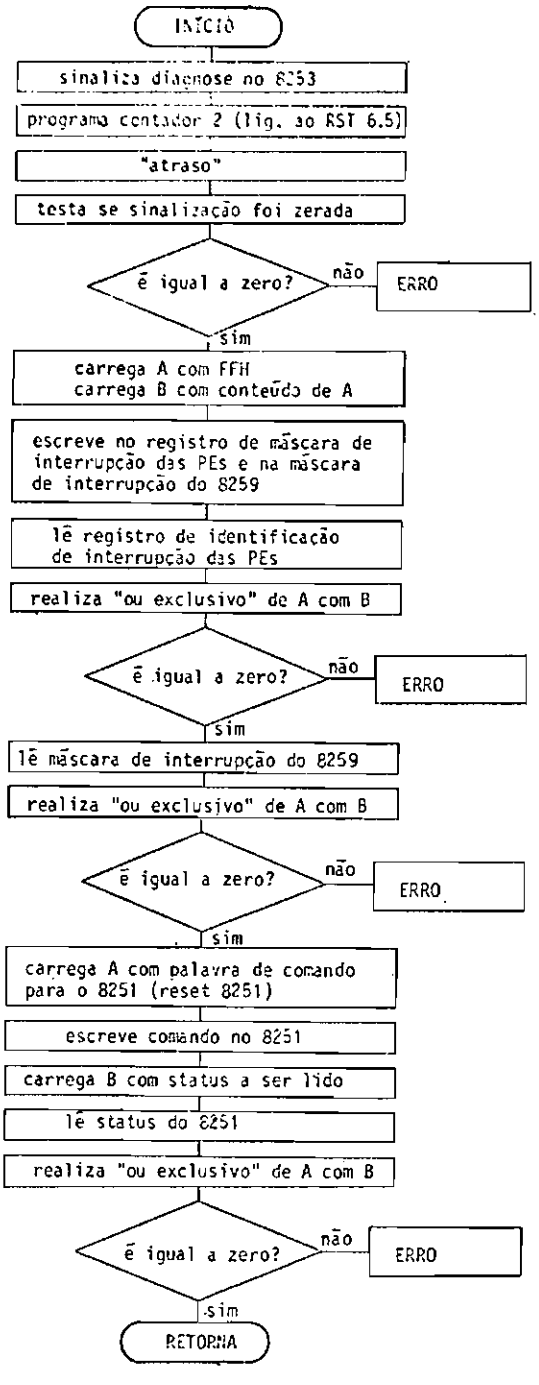


Fig. B.7 - Fluxograma da sub-rotina de teste de periféricos do Supervisor.

B.2 - ROTINA DE AUTODIAGNOSE DA PORTA EXTERNA

A rotina de autodiagnose de PE utiliza todas as sub-rotinas que compoẽm a rotina de autodiagnose do SV. Pequenas alteraçôes são necessárias na sub-rotina que testa os periféricos, pois a PE possui o CI 8273 que implementa a interface serial e que deve ser testado.

Cabe ao SV disparar periodicamente a autodiagnose na PE, atravẽs de comandos enviados pelo MCRBUS. Os resultados obtidos são analizados pelo próprio SV, daí a necessidade de reportar o "status" obtido na autodiagnose.

O fluxograma da rotina de autodiagnose da PE é mostrado na Figura B.8.

Os fluxogramas das sub-rotinas utilizadas na rotina de autodiagnose de PE são idênticos aos fluxugramas apresentados para o SV, a exceção da sub-rotina de teste dos periféricos, que tem seu fluxograma mostrado na Figura B.9.

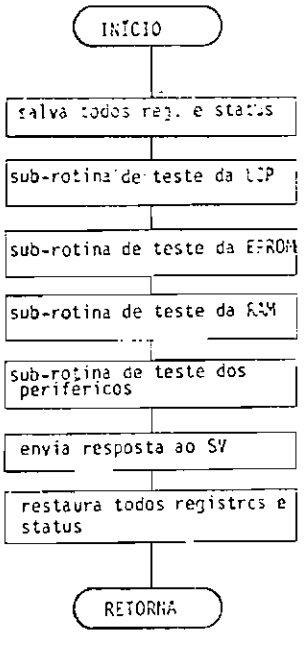


Fig. B.8 - Fluxograma da rotina de autodiagnose da Porta Externa.

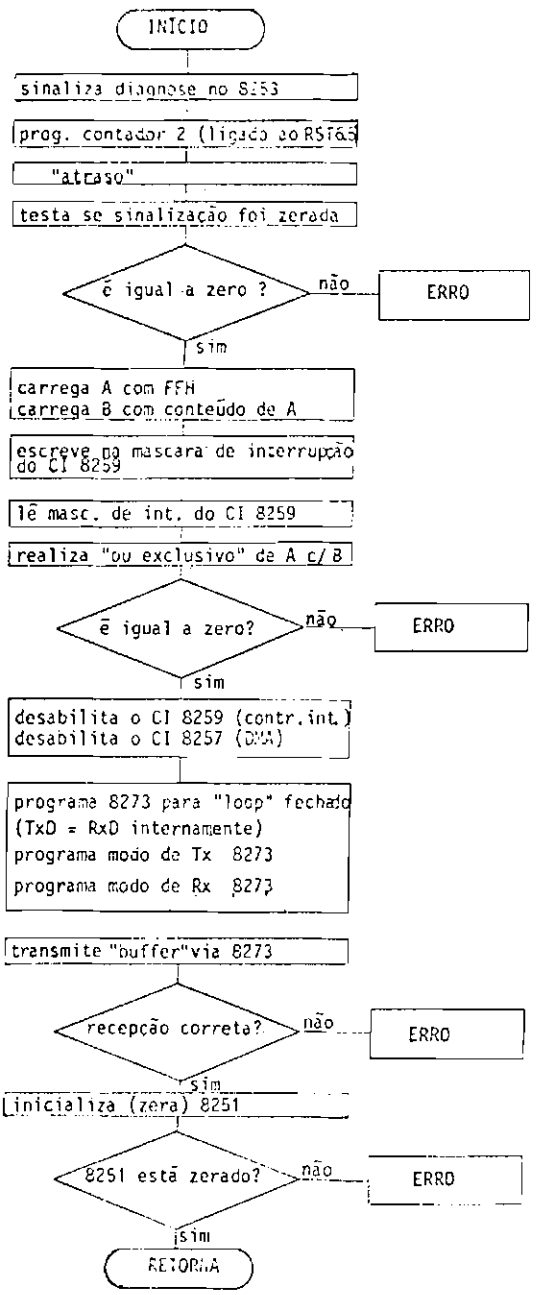


Fig. B.9 - Fluxograma da sub-rotina de teste dos periféricos da Porta Externa.

APÊNDICE C

DESCRIÇÃO DAS INTERFACES COM O "ÁRBITRO" e "CHAVE DIGITAL" E APRESENTAÇÃO DOS CIRCUITOS DESTES MÓDULOS

C.1 - ÁRBITRO

A conexão física SVs"árbitro" é feita através de cabo do tipo "flat-cable" que parte dos SVs para o "árbitro". A conexão física SVs-MCRBUS, com a utilização do "árbitro", continua sendo feita pelo "back plane" do gabinete que abriga o MCR.

O circuito do "árbitro" tem como proposta estar fisicamente contido na mesma placa que contém o circuito da PI, embora trabalhe de forma independente dele. Desta maneira, a conexão SVs-PI é feita através dos cabos que fazem a conexão SVs-"árbitro".

A proposta de acondicionar PI + "árbitro" na mesma placa implica algumas mudanças no conjunto que forma os módulos SV + PI, o qual é composto pela placa CPUpadrão + placa Unidade PI (total de 2 placas). Com esta nova proposta, PI + "árbitro" ocupam 1 placa, e cada SV ocupa 1 placa, perfazendo um total de 3 placas para o conjunto PI+ "árbitro" e 2 SVs.

Este esclarecimento é pertinente no que diz respeito à implementação física da arquitetura proposta no Capítulo 4 deste trabalho, pois para efeito das análises a PI não foi considerada.

Os sinais necessários para a conexão SVs-PI são um subconjunto dos sinais que compõem a via de conexão SVs-"árbitro". A conexão SVs-MCRBUS é feita através do "back plane" do MCR. Cabe ao "árbitro" controlar o acesso dos SVs à PI e ao MCRBUS. O controle de acesso ao MCRBUS é feito através de liberação de portas de alta impedância localizadas nos próprios SVs, enquanto o controle de acesso à PI é feito através da liberação de portas de alta impedância localizadas no "árbitro".

Os sinais utilizados para conectar cada um dos SVs ao "árbitro são:

D0 - D7: Dados

A0 - A15: Endereços.

I/OR,I/OW,MEMR,MEMW: Pulsos de leituras e escrita.

RESET OUT: "Reset" (inicialização) utilizado pelo "árbitro" como sincronismo para evitar que o sinal ARBRESET atue nas PEs.

ARBRESET: "Reset" (inicialização) gerado pelo "árbitro" conectado ao RESET IN da UCP 8085-A do SV.

CLOCK OUT: Saída de relógio gerada pela UCP 8085-A. O sinal de relógio (CLOCK OUT) gerado pelo SV1 é utilizado pelo "árbitro" para prover sincronismo na geração do sinal que indica o momento em que a comparação a ser executada entre os barramentos de dados é válida.

ARBCLOCK: Relógio (CLOCK) gerado pelo "árbitro", conectado à entrada de relógio (X1 e X2) da UCP 8085 do SV.

RESDIAG: Resultado da autodiagnose emitido pelo SV para o "árbitro". Caso o resultado "0", isto indica que houve erro, e caso seja "1" indica que não houve erro detetado na autodiagnose.

HABSV: Habilita SV, gerado pelo "árbitro" para habilitar desabilitar a conexão do SV ao MCRBUS. Este sinal controla a liração das portas de alta impedância no SV, as quais estão ligados os sinais do MCRBUS. Todos os sinais do MCRBUS têm conexão liberada com o SV ativo. No caso do SV reserva

estão liberadas as conexões dos sinais unidirecionais do MCRBUS que têm o sentido MCRBUS → SV. Inclui-se neste caso o barramento de dados, quando o sentido da transferência for MCRBUS→ SV. No sentido contrário, SV → MCRBUS, o SV reserva tem a conexão do barramento de dados bloqueadas;

TRAP: "Trap", sinal gerado pelo "árbitro", conectado à entrada TRAP da UCP 8085-A do SV. Utilizado para disparar a rotina de autodiagnose no SV em caso de deteção de erro na comparação dos sinais dos barramentos de dados dos dois SVs. Uma vez disparada a autodiagnose, o "árbitro" desconecta o SV do MCRBUS. A conexão só é feita novamente caso o sinal RESDIAG determine a não-deteção de erro pela autodiagnose.

Do grupo de sinais descritos são os seguintes que fazem parte da conexão SVs-PI:

D0-D7: que são liberados em ambos os sentidos para o SV ativo, e apenas no sentido PI → SV para o SV reserva;

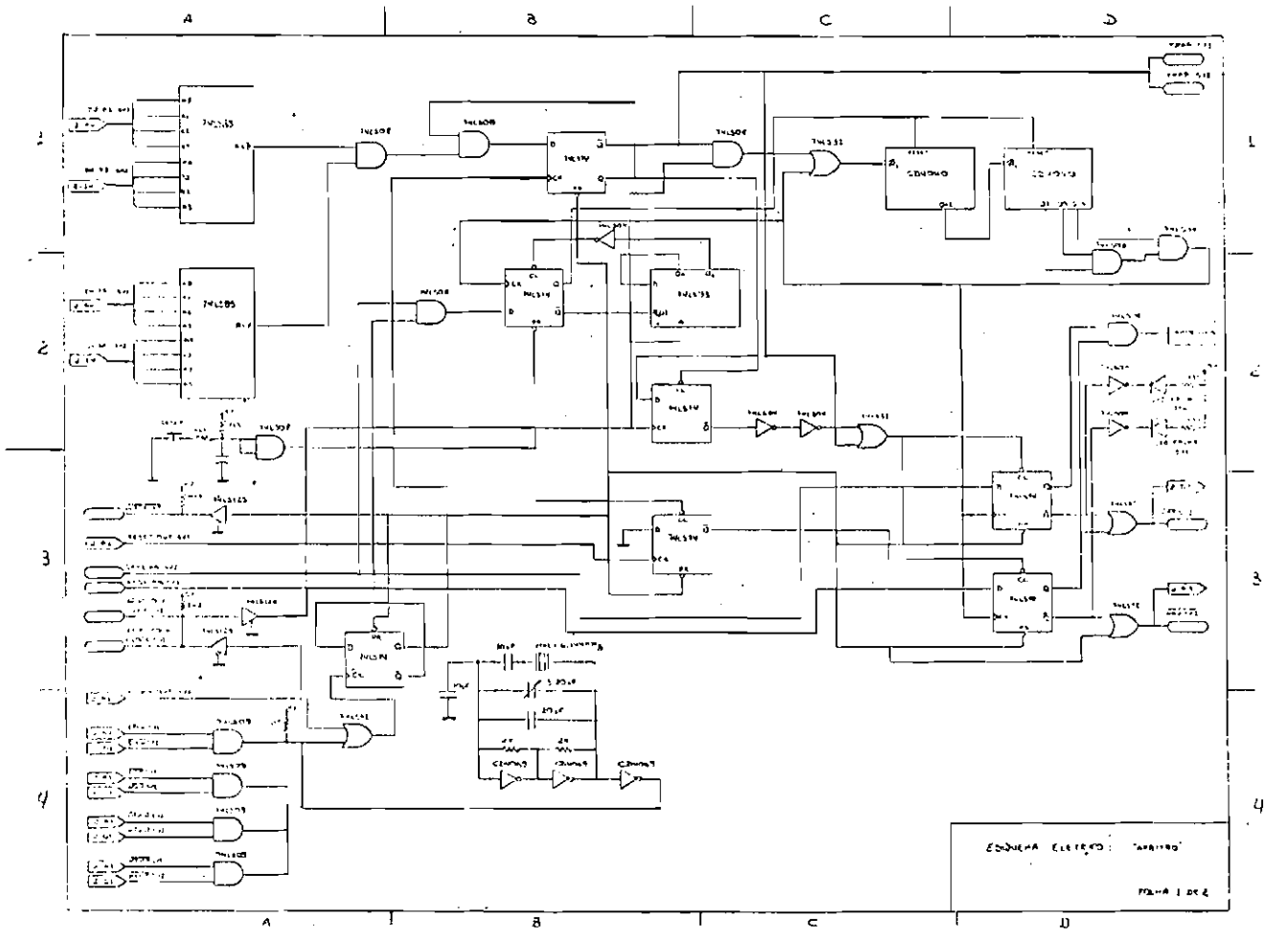
A0-A15: liberados somente para o SV ativo;

I/OR,I/OW, MEMR, MEMW: liberados para o SV ativo;

RESET OUT: liberado para o SV ativo;

e CLOCK OUT: liberado para o SV ativo.

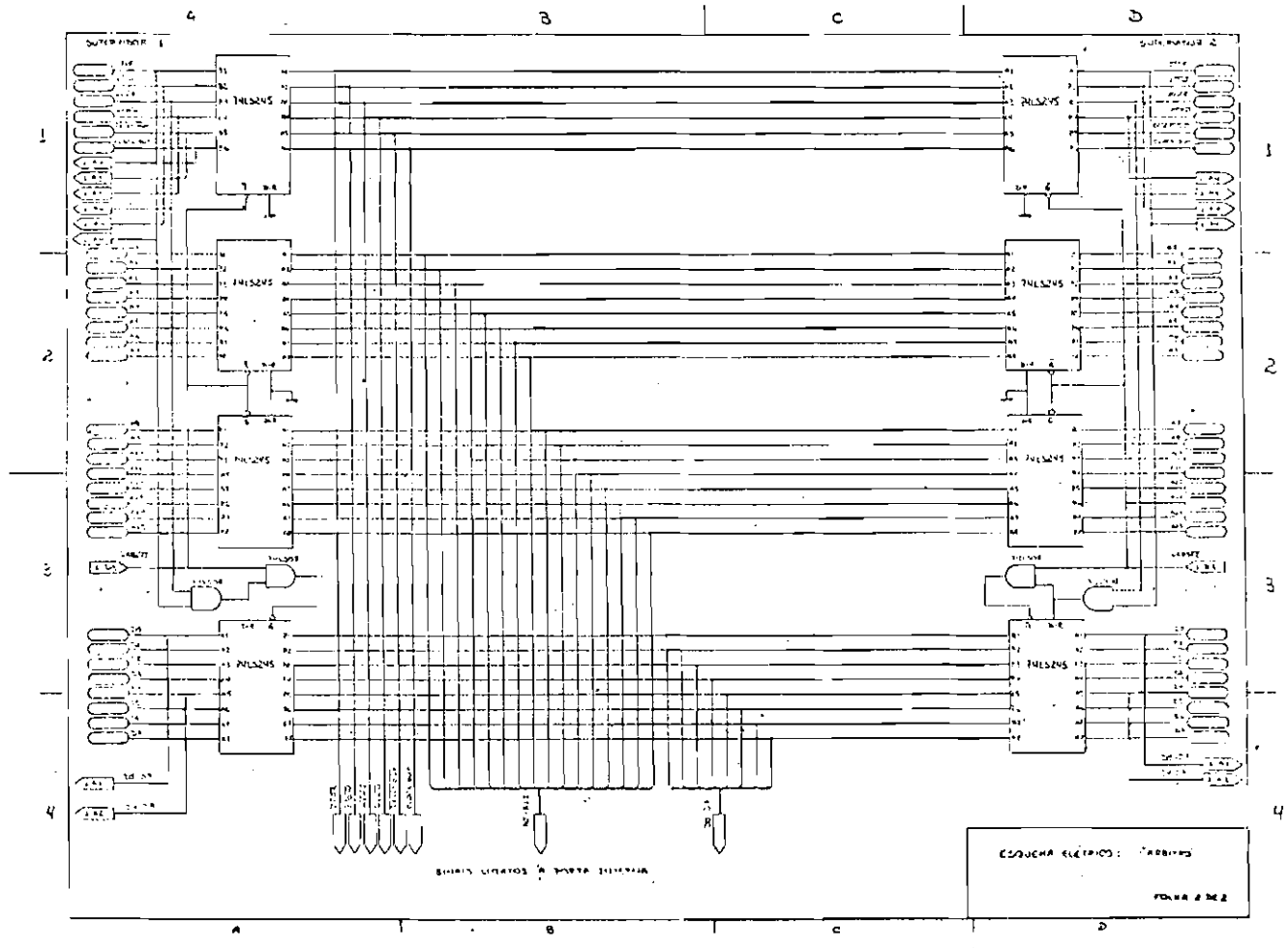
O esquema elétrico do "árbitro" é mostrado nas duas folhas seguintes através de uma redução do desenho original, feito em papel A3.



(continua)

Fig. C.1 - Esquema elétrico "ÁRBITRO"

Fig. C.1 - Conclusão.



C.2 - CHAVE DIGITAL

A conexão física SV-"chave digital" é feita pelo MCRBUS, ao qual a "chave digital" está conectada. Os sinais utilizados são:

WRSV: Pulso de escrita gerado pelo SV ativo para indicar operação de escrita através do MCRBUS.

A0-A5: Endereços gerados pelo SV ativo e decodificados na "chave digital" para selecionar qual a configuração à ser considerada. Esta decodificação ocorre quando é gerado o pulso WRSV em conjunto com os endereços atribuídos à "chave digital".

Os endereços existentes no MCRBUS são endereços de portas de E/S do SV e estão distribuídos da seguinte forma:

40H-47H: PE1

48H-4FH: PE2

50H-57H: PE3

58H-5FH: PE4

60H-67H: PE5

68H-6FH: PE 6

70H-77H: PE 7

78H-7FH: sincronismo/controles.

A "chave digital" adota os endereços destinados à PE7, que uma vez decodificados durante o pulso WRSV, tem o seguinte significado:

END 70H: PE reserva assume a linha serial conectada à PE1; as demais PEs permanecem ligadas a suas respectivas linhas.

END 71H: PE reserva assume a linha serial conectada à PE2, as demais PEs permanecem conectadas as suas respectivas linhas.

END 72H: PE reserva assume a linha serial conectada à PE3, as demais PEs permanecem conectadas as suas respectivas linhas.

END 73H: PE reserva assume a linha serial conectada à PE4, as demais PEs permanecem conectadas as suas respectivas linhas.

ENDEREÇOS: 74H, 75H, 76H e 77H: As PEs permanecem ligadas as suas respectivas linhas.

Os sinais da interface serial de cada PE são conectados à "chave digital" que, por sua vez, realiza adequadamente a conexão com as linhas externas. Estes sinais são:

CD, CTS, TxC, RxC, RxD: entradas na interface serial.

RTS, TxD: saídas na interface serial.

Cada PE, inclusive a reserva, possui um cabo que liga estes sinais à "chave digital".

O esquema elétrico da "chave digital" é mostrado na folha seguinte através de uma redução do desenho original, feito em papel A3.

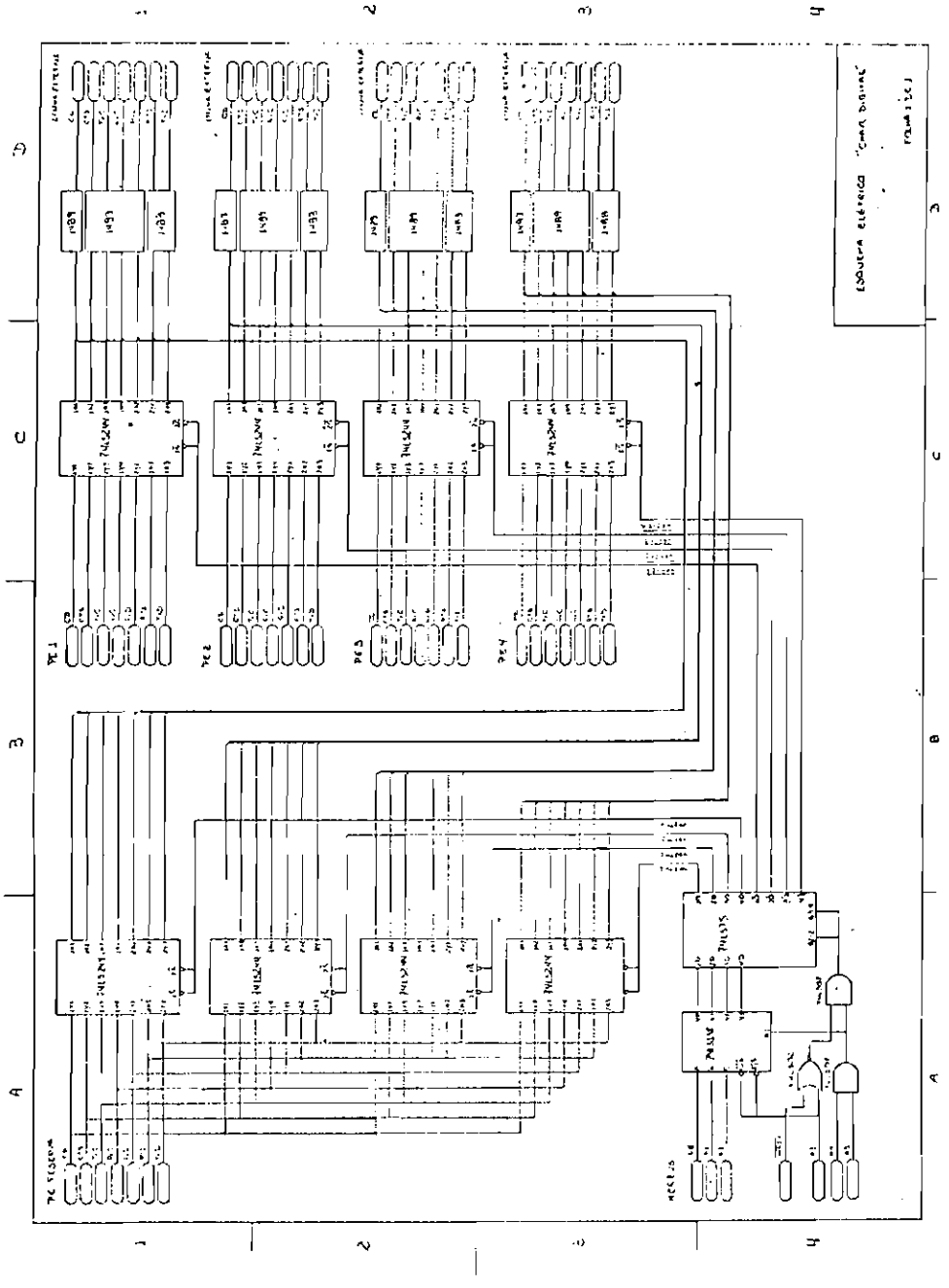


Fig. C.2 - Esquema elétrico "CHAVE DIGITAL".

APÊNDICE D

DISPONIBILIDADE DO EQUIPAMENTO MCR VARIANDO O NÚMERO DE PORTAS EXTERNAS

O equipamento MCR pode ser configurado com um número variável de Portas Externas (PEs), de acordo com as necessidades de sua aplicação. No texto deste trabalho foi considerado o número de PEs igual a 4, visto que é a configuração mais usual.

Neste apêndice são apresentados os valores obtidos para a disponibilidade do MCR com diferentes números de PEs, tanto para arquitetura atual como para a arquitetura proposta.

Para os cálculos efetuados consideraram os valores das taxas de falhas obtidas no Apêndice A e a mesma taxa média de reparos para todas as placas do MCR.

Dois critérios de manutenção foram observados ao se obter a taxa média de reparos e, desta meneira, foram obtidos dois valores de disponibilidade para cada configuração; cada um considerando um critério de manutenção. Estes critérios são:

CRITÉRIO 1 - Substituição de placas defeituosas em caso de falhas, o que resulta em um tempo médio para manutenção de 30 minutos (0,5 h). Neste caso a taxa média de reparos é 1/tempo médio de reparo, onde "tempo médio de reparo" é igual à soma do "tempo médio de espera" com o "tempo médio para manutenção"; ou seja , "tempo médio de reparo "= 5h + 0,5h,

μ_{MCR} = 1/5,5h = 181818,18 r/10^6h, sendo que o tempo médio de espera foi obtido no Capítulo 3, seção 3.2,

CRITÉRIO 2 - Manutenção das placas defeituosas em caso de falhas, o que implica um tempo médio para manutenção de 7h. Neste caso a taxa média de reparos é dada por μ_{MCR} = 1/12h = 83333,3 r/10^6h.

D.1 - CÁLCULO DA DISPONIBILIDADE PARA A ARQUITETURA ATUAL

O cálculo de disponibilidade para a arquitetura atual é feito utilizando o modelo apresentado no capítulo 3, seção 3.2, sendo considerando os casos de uso de componentes comerciais e uso de componentes mais confiáveis. Os valores obtidos para a disponibilidade são mostrados nas Tabelas D.1 (componentes comerciais) e D.2 (componentes mais confiáveis).

D.2 - CÁLCULO DA DISPONIBILIDADE PARA ARQUITETURA PROPOSTA

Os cálculos de disponibilidade para a arquitetura proposta foram feitos para um mínimo de 2 PEs (1 PE ativa a 1 reserva) e um máximo de 7 PEs (6 PEs ativas e 1 PE reserva). Para tanto, a "chave digital" teve sua capacidade acrescida de forma a atender o caso máximo de 7 PEs, sendo que a taxa de falhas obtida para seu circuito foi λ_{CD} =23,9005 f/10^6hs.

O diagrama de transição de estados para o caso de "K" PEs (2 < K < 7) é mostrado na Figura D.1.

As taxas de transição indicadas no diagrama de transição de estados são:

λ_{SVP} = 227,2922 f/10^6h,

λ_{PE_P} = 421,727 f/10^6h,

$\lambda_N = \lambda_{ARB} + \lambda_{CD}$ = (19,0533 + 23,9005) f/10^6 h= 42,9538 f/10^6h,

μ = 181818,18 r/10^6h ou

μ = 83333,3 r/10^6h.

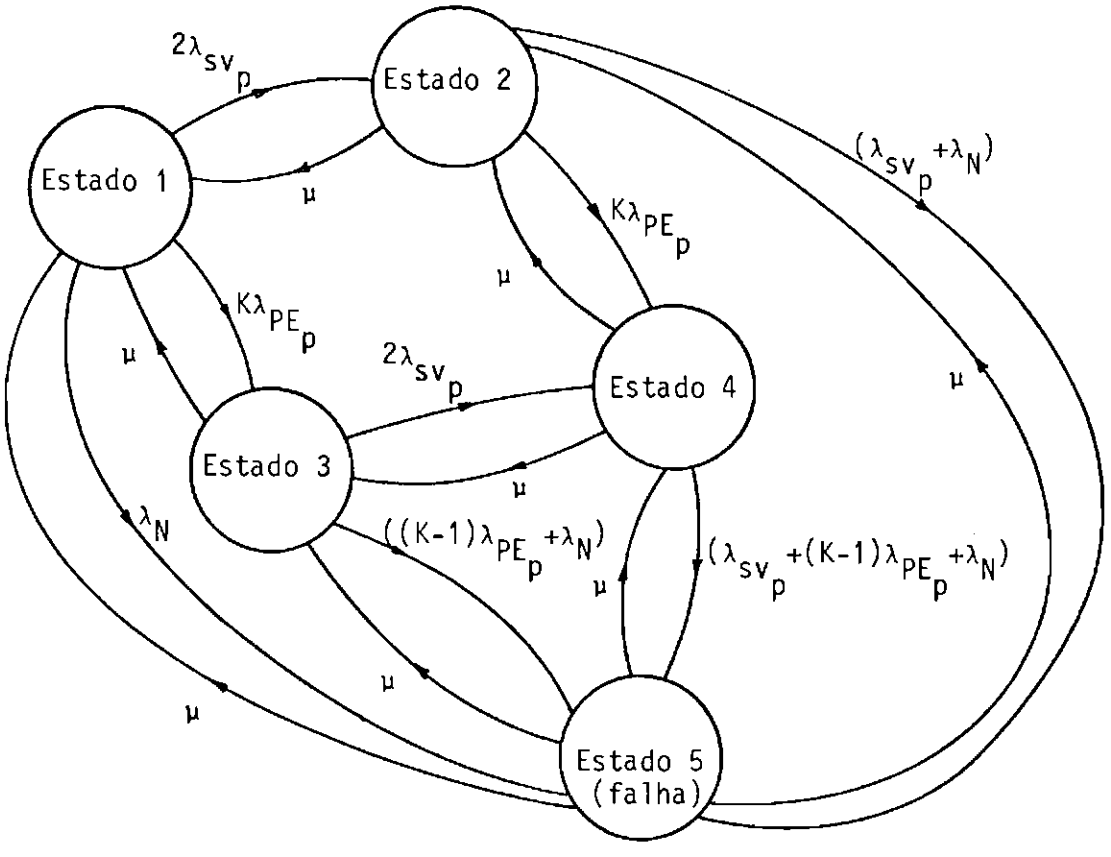


Fig. D.1 - Diagrama de transição de estados para o caso de "K" PEs.

A partir do diagrama da Figura D.1 e suas transições, foi levantada a matriz de taxa de transição de estados, mostrada a seguir:

$$\underline{A} = \begin{bmatrix} (1-2\lambda_{SV_p} - 5\lambda_{PE_p} - \lambda_N) & 2\lambda_{SV_p} & 5\lambda_{PE_p} & 0 & \lambda_N \\ \mu & (1-\mu - \lambda_{SV_p} - \lambda_N - 5\lambda_{PE_p}) & 0 & 5\lambda_{PE_p} & \lambda_{SV_p} + \lambda_N \\ \mu & 0 & (1-\mu - 2\lambda_{SV_p} - 4\lambda_{PE_p} - \lambda N) & 2\lambda_{SV_p} & 4\lambda_{PE_p} + \lambda_N \\ 0 & \mu & \mu & (1-2\mu - \lambda_{SV_p} - 4\lambda_{PE_p} - \lambda_N) & \lambda_{SV_p} + 4\lambda_{PE_p} + \lambda_N \\ \mu & \mu & \mu & \mu & (1-4\mu) \end{bmatrix}$$

Utilizando os mesmos critérios apresentados no Capítulo 4, Seção 4.3, são obtidos os valores do parâmetro disponibilidade da arquitetura proposta para diversas configurações (variando o número de PEs). Estes valores são mostrados na Tabela D.3.

TABELA D.1

DISPONIBILIDADE PARA A ARQUITETURA ATUAL COM O USO DE COMPONENTES COMERCIAIS

Nº PEs	DISPONIBILIDADE		INDISPONIBILIDADE	
	CASO 1	CASO 2	CASO 1	CASO 2
1	99,64%	99,23%	$3,56.10^{3}$	$7,74.10^{3}$
2	99,41%	98,73%	$5,87.10^{3}$	$1,27.10^{2}$
3	99,18%	98,24%	$8,16.10^{3}$	$1,76.10^{2}$
4	98,96%	97,75%	$1,04.10^{2}$	$2,25.10^{2}$
5	98,73%	97,27%	$1,27.10^{2}$	$2,73.10^{2}$
6	98,50%	96,79%	$1,49.10^{2}$	$3,21.10^{2}$
7	98,28%	96,32%	$1,72.10^{2}$	$3,68.10^{2}$

OBS.: CASO 1 : $\mu_{MCR} = 181818,18\ r/10^{6}h$

CASO 2 : $\mu_{MCR} = 83333,3\ r/10^{6}h$.

TABELA D.2

DISPONIBILIDADE PARA A ARQUITETURA ATUAL COM O USO DE COMPONENTES MAIS CONFIÁVEIS

Nº PEs	DISPONIBILIDADE		INDISPONIBILIDADE	
	CASO 1	CASO 2	CASO 1	CASO 2
1	99,89%	99,76%	$1,10.10^{3}$	$2,39.10^{3}$
2	99,83%	99,62%	$1,73.10^{3}$	$3,76.10^{3}$
3	99,77%	99,49%	$2,35.10^{3}$	$5,11.10^{3}$
4	99,70%	99,35%	$2,97.10^{3}$	$6,46.10^{3}$
5	99,64%	99,22%	$3,59.10^{3}$	$7,81.10^{3}$
6	99,58%	99,09%	$4,22.10^{3}$	$9,15.10^{3}$
7	99,52%	98,95%	$4,84.10^{3}$	$1,05.10^{2}$

OBS.: CASO 1 : μ_{MCR} = 181818,18 r/10^{6}h
CASO 2 : μ_{MCR} = 83333,3 r/10^{6}h

TABELA D.3

DISPONIBILIDADE PARA A ARQUITETURA PROPOSTA COM O USO DE COMPONENTES COMERCIAIS

Nº PEs	DISPONIBILIDADE		INDISPONIBILIDADE	
	CASO 1	CASO 2	CASO 1	CASO 2
2	99,99%	99,99%	6,12.10	1,42.10
3	99,99%	99,98%	6,66.10	1,68.10
4	99,99%	99,98%	7,46.10	2,05.10
5	99,99%	99,97%	8,52.10	2,55.10
6	99,99%	99,97%	9,84.10	3,16.10
7	99,99%	99,96%	1,14.10	3,88.10

OBS.: CASO 1 : μ_{MCR} = 181818,18 r/10^{6}h
CASO 2 : μ_{MCR} = 83333,3 r/10^{6}h