1. Publicação nº	2. Versão	3. Data	5. Distribuição
INPE-3798-PRE/893		*Fev., 1986*	☐ Interna ☒ Externa ☐ Restrita

4. Origem	Programa
DCA/DIA	*SUBORD*

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

COMPUTADOR DE BORDO, TOLERÂNCIA A FALHAS
SUPERVISÃO DE BORDO, SISTEMAS DE PROCESSAMENTO DISTRIBUÍDO

7. C.D.U.: *681.31*

8. Título *INPE-3798-PRE/893*

ASPECTOS DE TOLERÂNCIA A FALHAS DO COMPUTADOR DE BORDO ASTRO B/3

10. Páginas: *11*

11. Última página: *10*

12. Revisada por

Ricardo de A. Mendes

9. Autoria *Alderico Rodrigues de Paula Jr.*

Assinatura responsável

13. Autorizada por

Marco Antonio Raupp
Diretor Geral

14. Resumo/Notas

A arquitetura do computador de bordo ASTRO B/3 é apresenta da. Para garantir que qualquer defeito simples interno ao ASTRO B/3 seja recuperado automaticamente, diversos mecanismos de tolerância a falhas foram incorporados. As técnicas de tratamento de falhas foram organizadas em níveis hierárquicos. Ao nível de unidade de processamento essas técni cas foram divididas em processos aplicativos, sistema operacional e cir cuito. Os mecanismos de detecção, análise e recuperação ao nível de cir cuito são discutidos.

15. Observações

Este trabalho deverá ser apresentado no I Simpósio em Sistemas de Com putadores Tolerantes a Falhas.

ASPECTOS DE TOLERÂNCIA A FALHAS DO COMPUTADOR DE BORDO ASTRO B/3

Alderico R. de Paula Jr.*

RESUMO

A arquitetura do computador de bordo ASTRO B/3 é apresentada. Para garantir que qualquer defeito simples interno ao ASTRO B/3 seja recuperado automaticamente, diversos mecanismos de tolerância a falhas foram incorporados. As técnicas de tratamento de falhas foram organizadas em níveis hierárquicos. Ao nível de unidade de processamento essas técnicas foram divididas em processos aplicativos, sistema operacional e circuito. Os mecanismos de detecção, análise e recuperação ao nível de circuito são discutidos.

ABSTRACT

The architecture of the on board computer ASTRO B/3 is presented. To assure that any internal single-point fault is automatically recovered, fault tolerance techniques were utilized in the design. These techniques were organized into logical hierarchical layers. At the processing unit layer, the detection, analysis and recovery techniques are divided into three layers: applicative process, operating system and hardware. The error handling techniques at the hardware layer are dicussed.

INTRODUÇÃO

O computador de bordo ASTRO B/3 está sendo desenvolvido para supervisão e controle dos satélites da Missão Espacial Completa Brasileira (MECB). As principais tarefas a serem executadas pelo ASTRO B/3 são:

a) Adquirir os dados dos diversos sensores a bordo do satélite, processá-los, formatá-los e enviá-los para as estações terrenas.

b) Receber os pacotes de telecomandos provenientes das estações terrenas, decodificá-los e atuar nos diversos subsistemas do satélite.

---

*Departamento de Engenharia de Computação em Aplicações Espaciais - Instituto de Pesquisas Espaciais - INPE; Caixa Postal 515; 12200 - São José dos Campos - SP

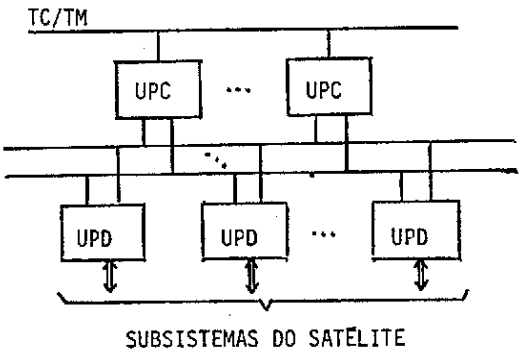
c) Supervisionar os diversos subsistemas do satélite, detectar falhas e realizar as medidas corretivas preestabelecidas.

Dado que o computador de bordo é um subsistema essencial para a operação do satélite, uma falha do computador poderá tornar o satélite inoperante. Para evitar que defeitos simples internos ao computador perturbem a operação do satélite, mecanismos de tolerância a falhas foram nele incorporados. Devido às limitações de peso e energia, a redundância ao nível de circuito foi minimizada ao máximo possível.

Neste trabalho, inicialmente será apresentada a arquitetura selecionada para o ASTRO B/3. Em seguida, será discutida a metodologia utilizada para o tratamento de falhas e, finalmente, serão descritos os mecanismos de tratamento de falhas incorporados ao nível de circuito.

PADRÃO INPE DE SUPERVISÃO DE BORDO

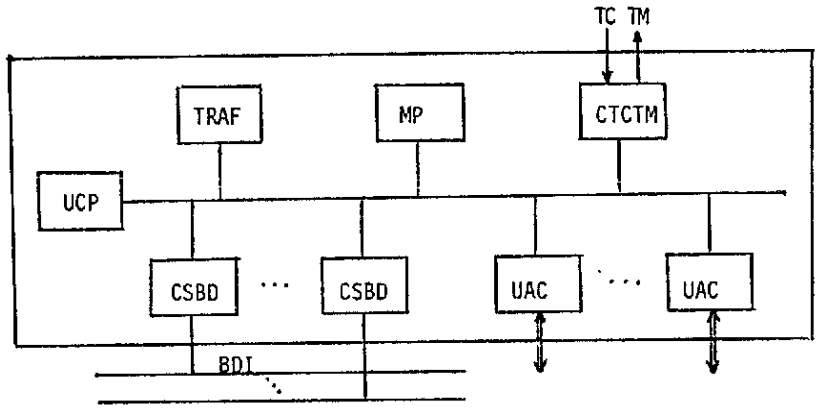
A arquitetura selecionada para o ASTRO B/3 está baseada no Padrão INPE de Supervisão de Bordo - PISB - (PAULA JÚNIOR et alii - 1984a).O PISB define um sistema de computação distribuído, no qual as unidades de processamento são organizadas em dois níveis hierárquicos. As unidades de processamento de níveis superiores têm a função de supervisionar o sistema e comunicar-se com as estações terrenas, enquanto as unidades de níveis inferiores são dedicadas à aquisição de dados e ao controle dos subsistemas. As unidades de processamento são interconectadas por barramentos seriais redundantes de comunicação de dados (Figura 1).



UPC Unidade de Processamento e Comunicação
UPD Unidade de Processamento Distribuído
BDI Barramento de Dado Interno
TC/TM Telecomando e Telemetria

Fig. 1 - Padrão INPE de supervisão de bordo.

As unidades de processamento são constituídas de módulos básicos que são a elas incorporados em função dos requisitos da aplicação (Figura 2).



UCP Unidade Central de Processamento
TRAF Tratamento de Falhas
MP Memória Principal
CTCTM Comunicador Serial de Telecomando e Telemetria
CSBD Comunicador Serial de Barramento de Dados
UAC Unidade de Aquisição e Controle

Fig. 2 - Unidade de processamento do PISB.

A Unidade Central de Processamento (UCP) é baseada no microprocessador de 16 bits SBP9989, o qual é fabricado com tecnologia I^2L e caracterizado pela alta resistência à radiação cósmica e pelo baixo consumo de energia. Além do microprocessador a UCP comporta o relógio de bordo e os circuitos de tratamento de interrupções.

A Memória Principal é constituída de um a oito módulos de memória de acesso aleatório (RAM) de 4Kx22 e de memória de leitura (ROM) de 4Kx16. As palavras que são armazenadas nos módulos RAM são codificadas segundo o código de Hamming modificado, o qual permite a detecção de erros duplos e a correção de erros simples. Os circuitos para detecção e correção de erros da RAM, bem como o circuito de cão-de-guarda, estão localizados no módulo de Tratamento de Falhas (TRAF).

O Comunicador Serial de Telecomando e Telemetria (CSTCTM) recebe os pacotes de telecomandos provenientes das estações terrenas detectando o sincronismo e a consistência dos dados recebidos. Este módulo envia para as estações terrenas os pacotes de telemetria gerando uma palavra de sincronismo e uma de código CRC.

O Comunicador Serial de Barramento de Dados (CSBD) modula as palavras a serem enviadas para as outras unidades de processamento no código "Bi-phase" e acrescenta um bit de paridade. Ao receber palavras de outras unidades de processamento, o CSBD demodula as palavras recebidas e verifica a consistência dos dados recebidos.

A Unidade de Aquisição e Controle (UAC) fornece os sinais de controle para os subsistemas do satélite e adquire os dados dos diversos subsistemas na forma analógica ou digital. Os dados analógicos são convertidos em digitais por um conversor A/D interno à Unidade de Aquisição.

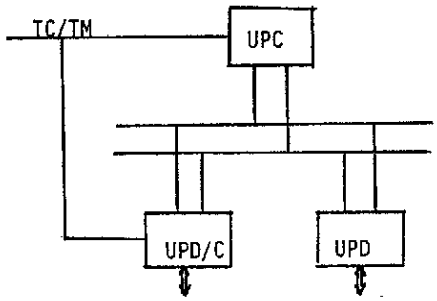
ARQUITETURA DO ASTRO B/3

Devido ao fato de a confiabilidade requerida para o ASTRO B/3 não ter sido estabelecida a priori, as seguintes regras básicas foram definidas como requisitos básicos:

1) O computador de bordo deverá recuperar-se automaticamente de qualquer defeito interno simples.
2) Após o lançamento do mastro, o que deverá ocorrer nos primeiros dias em órbita, o computador não deverá executar nenhuma tarefa crítica. Portanto, um pequeno atraso na execução de uma tarefa ou alguns erros esporádicos do computador não deverão tornar o satélite inoperante.
3) A redundância adicional, ao nível de circuito deverá ser a mínima possível.

Dados os requisitos descritos para o ASTRO B/3 não se justifica a utilização de redundânica tripla modular ou mesmo a utilização de duas unidades para executar a mesma tarefa. Portanto, todas as tarefas poderão ser executadas em apenas uma unidade de processamento sob a supervisão de uma unidade externa. Com base nas especificações preliminares foi constatado que duas unidades de processamento são suficientes para executar todas as tarefas de bordo.

A arquitetura selecionada para o ASTRO B/3 com base na PISB e que satisfaz os requisitos definidos é apresentada na Figura 3.



UPC Unidade de Processamento e Comunicação
UPD/C Unidade de Processamento Distribuído e Comunicação
UPD Unidade de Processamento Distribuído

Fig. 3 - Arquitetura selecionada para o ASTRO B/3.

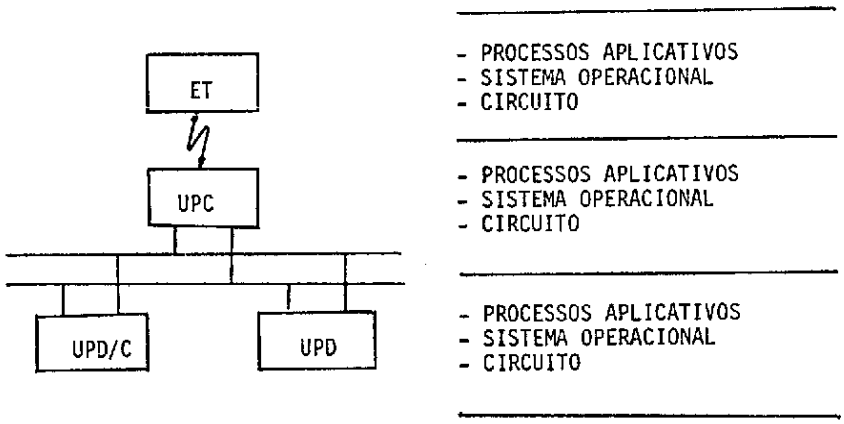
Durante a operação normal do ASTRO B/3 a UPC realiza a supervisão do sistema e as comunicações com as estações terrenas, enquanto a UPD/C fornece os sinais de controle para os subsistemas e realiza a aquisição de dados. Durante este estado, a UPD fica desligada para não dispender energia.

Em caso de falha da UPC, a UPD/C assume as tarefas da UPC e energiza a UPD, a qual passará então a executar a aquisição de dados e o controle dos subsistemas. Se a primeira unidade a falhar for a UPD/C, a UPD é energizada e assume as tarefas da UPD/C. Em caso de falha da UPC e UPD a UPD/C deverá continuar operando de forma degradada.

Para detectar falhas nas unidades de processamento, diversos mecanismos foram incorporados e serão discutidos nas próximas seções.

METODOLOGIA PARA TRATAMENTO DE FALHAS

Para facilitar a implantação dos mecanismos de tratamento de falhas no ASTRO B/3, estes foram organizados em níveis hierárquicos (Paula Júnior e Martins, 1984b conforme apresentado na Figura 4.



ET Estação Terrena
UPC Unidade de Processamento e Comunicação
UPD/C Unidade de Processamento Distribuído e Comunicação
UPD Unidade de Processamento Distribuído

Fig. 4 - Organização dos mecanismos de tratamento em níveis hierárquicos.

Em cada nível hierárquico os mecanismos de tratamento de falhas são divididos em detecção, análise e recuperação. Para evitar interpretação incorreta, os termos defeito, erro e falha terão as seguintes interpretações neste trabalho:

Defeito - é um mal funcionamento de um circuito ou uma imperfeição de um algoritmo que pode causar um erro.

Erro - é um item na estrutura da informação que quando processado por um algoritmo normal, produz uma falha.

Falha - é um desvio externo do comportamento especificado para o sistema.

O defeito pode ser transiente ou permanente. Pode ser causado por um fenômeno físico ou por imperfeições no projeto dos circuitos e programas. Um defeito pode ficar num estado latente por um certo período de tempo, ou então afetar itens da estrutura de dados ou do estado do sistema causando erros simples ou múltiplos. Tais erros podem ser detectados e confinados ao nível em que foram gerados, ou então se propagar para níveis superiores e se multiplicar. Estes erros podem ser detectados em algum nível superior ou então gerar informações ou atuações errôneas, causando uma falha no sistema.

Após a detecção de um erro, a análise para determinar a causa do erro ou para localizar o defeito pode ser realizada no mesmo nível em que o erro foi detectado ou em níveis superiores. O mesmo ocorre com a recupera

ção. Em geral, os mecanismos de detecção, análise e recuperação são executados em mais de um nível e de forma cooperativa.

Neste trabalho serão discutidos principalmente os mecanismos de tratamento de falhas ao nível de circuito. Os mecanismos ao nível de sistema operacional são apresentados com maiores detalhes em outros trabalhos (ver por exemplo (Alonso et alii, 1985).

MECANISMOS DE TRATAMENTO DE FALHAS AO NÍVEL DE CIRCUITO

Devido à limitação de peso e energia, procurou-se incorporar às unidades de processamento o menor número possível de circuitos adicionais. Sendo a memória o módulo mais susceptível às radiações cósmicas, foi nele incorporada a maioria dos circuitos adicionais.

A Memória Principal foi dividida em oito regiões de 4K palavras. Cada região pode ser ocupada por módulos de memória do tipo RAM ou ROM e protegida contra a escrita por um circuito de máscara controlado pelo sistema operacional. Para evitar que defeitos nos programas não possam ser corrigidos após o lançamento do satélite optou-se por utilizar, sempre que possível, módulos de RAM.

Os módulos de RAM são formados por 22 circuitos de memória de 4K palavras por 22 bits. Os primeiros 16 circuitos de memória armazenam a palavra do processador, enquanto os demais armazenam os 6 bits de paridade do código de Hamming modificado. Tais bits são necessários para detecção de erros duplos e correção de erros simples. Nesta organização cada circuito de RAM contribui apenas para um bit da palavra lida da memória e, portanto, um defeito em apenas um circuito de RAM gera em erro simples.

Para a implantação do código de Hamming um circuito de detecção e correção de erros foi implantado no módulo TRAF. Durante o ciclo de escrita, ele gera os 6 bits de paridade, os quais são armazenados no mesmo endereço da palavra do processador. No ciclo de leitura, os 6 bits de paridade são gerados com base na palavra da memória e comparados com os bits de paridade lidos do mesmo endereço da memória. Em caso de erro simples a palavra lida da memória é corrigida, e o endereço armazenado é enviado às estações terrenas para análise. Quando um erro duplo é detectado, a unidade de

processamento é interrompida e a rotina para tratamento de falhas é chamada.

Como o módulo de ROM só é utilizado para a iniciação ou reiniciação do sistema, a detecção de defeitos nestes módulos é realizada antes da execução da rotina de iniciação através da verificação das palavras de "check sum" que estão inseridas neste módulo.

O Comunicador Serial de Barramento de Dados (CSBD) foi projetado de forma que as palavras transmitidas através do Barramento de Dados são recebidas e armazenadas no CSBD que as transmitiu. Isto permite que um protocolo ao nível de processo aplicativo compare a palavra que foi transmitida com a palavra original detectando desta forma os defeitos internos ao CSBD.

Dois métodos são utilizados para detectar erros no Barramento Interno de Dados. No primeiro, ao nível de circuito, o CSBD que transmite uma palavra gera um bit de paridade o qual é verificado no CSBD que o recebe. No segundo método, ao nível de processo aplicativo, a unidade de processamento que recebeu um arquivo de dados verifica a consistência do arquivo recebido. Caso nenhum erro seja detectado, uma confirmação é enviada à unidade de processamento que transmitiu o pacote.

No Comunicador Serial de Telecomando e Telemetria foi implementado um circuito que detecta a superposição de duas palavras recebidas e a inanição de dados no transmissor. Defeitos nesta unidade são detectados ao nível de processo aplicativo através dos protocolos de comunicação.

A comunicação de dados entre solo e bordo é realizada através de pacotes de dados. Para detectar erros no elo de comunicação solo/bordo, os dados a serem transmitidos são codificados utilizando o código cíclico redundante.

O método para detectar erros na Unidade de Aquisição e Controle consiste em verificar se os comandos enviados para os subsistemas do satélite foram executados através da leitura de sinais dos subsistemas que confirmam a execução desses comandos.

Para detectar erros na Unidade Central de Processamento (UCP) concomitantemente à operação, são necessários a duplicação da UCP e o uso de comparadores. Devido ao fato de ser muito grande a quantidade de circuitos necessários para duplicação e comparação, optou-se pela detecção de erros na UCP indiretamente, principalmente através de mecanismos ao nível de Sistemas Operacionais, tais como o de verificar se as tarefas foram concluídas com sucesso e no tempo previsto.

Um outro mecanismo utilizado para detecção de erros não-concomitantes à operação é o Cão-de-Guarda. A cada ciclo de operação, o Cão-de-Guarda deverá ser zerado pelo Sistema Operacional. Caso este evento não ocorra até uma vez e meia do ciclo de operação, o Cão-de-Guarda gera um pedido de interrupção não-mascarável. Se este pedido de interrupção não for atendido dentro do próximo ciclo de operação, o Cão-de-Guarda zera todo o sistema e o programa de iniciação é ativado. Este programa contém diversas rotinas de diagnose que verificam o estado do sistema. Decorrido um ciclo e meio após a reiniciação, se o Cão-de-Guarda não for zerado, um sinal de falha é gerado informando às outras unidades de processamento que esta unidade falhou de modo irrecuperável.

CONCLUSÕES

Um protótipo de laboratório contendo três unidades de processamento está em fase de conclusão no Departamento de Engenharia de Computação em Aplicações Espaciais (DCA) do Instituto de Pesquisas Espaciais. O sistema operacional está na fase de codificação e deverá ser implantado no protótipo de laboratório no início de 1986. Após a implantação do sistema operacional o ASTRO B/3 deverá passar por uma fase de validação. Neste período diversos defeitos serão gerados propositalmente com o objetivo de verificar a eficiência dos mecanismos de tratamento de falhas incorporados ao computador.

Em paralelo com as atividades de validação funcional do protótipo de laboratório, vem sendo desenvolvidas técnicas para o empacotamento de circuitos eletrônicos para aplicações espaciais. A técnica de empacotamento selecionada consiste na montagem de componentes do tipo "leadless chip carrier" sobre placas cerâmicas de camadas múltiplas. Esta técnica permite a redução da área de montagem de um para quatro em relação à montagem de

componentes do tipo "dual in line".

Após a validação do protótipo de laboratório, as três unidades de processamento serão empacotadas sobre placas cerâmicas e submetidas a testes de vibração e ciclos térmicos, tendo em vista a sua validação para aplicação em veículos espaciais. Subsequentemente aos testes ambientais deverá ser montada a versão de vôo do ASTRO B/3 que será utilizada nos satélites brasileiros. O primeiro satélite brasileiro controlado pelo computador de bordo ASTRO B/3 deverá ser colocado em órbita antes do final desta década.

REFERÊNCIAS BIBLIOGRÁFICAS

PAULA JR., A.R. et alii, "Síntese do Padrão INPE de Supervisão de bordo (PISB) Aplicação à MECB", Relatório Técnico INPE - 3111 - RTR/049, São José dos Campos, maio 1984a.

PAULA JR., A.R e MARTINS, R.C.O., "A Fault-Tolerant Multiprocessing Unit For On-Board Satellite Supervision and Control" 5º Congresso Brasileiro de Automática, Campina Grande, setembro 1984b.

ALONSO, J.D.D.; CINTRA, S.A.R.; MARTINS, R.C.O., "Tratamento de Erros por "Software" no Padrão INPE de Supervisão de Bordo". I Simpósio de Sistemas de Computadores Tolerantes a Falhas, São José dos Campos, setembro 1985.

INSTITUTO DE PESQUISAS ESPACIAIS; "Estudo de Viabilidade do Satélite Brasileiro - Documento Síntese"; Novembro 1979.